REPORT DOCUMENTATION PAGE

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	31 October 1997	Final 8/31/95 - 8/31/97

4. TITLE AND SUBTITLE

Multiple Access Low Probability of Intercept Networks

5. FUNDING NUMBERS

F49620-94-1-0023

6. AUTHOR(S)

Glenn E. Prescott

AFRL-SR-BL-TR-98-

0384

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Telecommunications & Information Sciences Laboratory
Department of Electrical Engineering & Computer Science
University of Kansas, Lawrence, KS 66045

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Air Force Office of Scientific Research /NM
110 Duncan Avenue
Bolling AFB, DC 20332

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

Distribution Unlimited

19980430 123

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE

13. ABSTRACT (Maximum 200 words)

Increased demands for communications in the tactical battlefield have fueled the development of multiple access low-probability-of-intercept networks. Most detectability studies of LPI networks have focused on the individual links of the network, in which the intercept and detectability calculations are conducted for a single network transmitter. The research reported here examines a different approach to network detectability analysis: It is assumed that the interceptor does not attempt to distinguish one emitter from another, but rather decides only if a network is operating or not. What distinguishes this approach from conventional link intercept analysis is that detection decisions are based on energy received from multiple sources.

Two network detection models are developed. A *dispersed network* intercept model is appropriate for scenarios in which the network transmitters are dispersed throughout a given tactical region, and the interceptor is inside the network. The interception area for the specified probabilities of detection and false alarm is used as a performance metric. A *stand-off network* intercept model is used for situations in which the network transmitters are collocated and the interceptor is standing-off. For this model, a network LPI quality factor is developed as a performance metric. Both models are developed for a frequency hopping code division multiple access network, using a wideband radiometer and filter band/binary moving window detector as potential intercept receivers.

14. SUBJECT TERMS

Low Probability of Intercept, LPI, Spread Spectrum, Communications Networks

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

DTIC QUALITY INSPECTED 8

Final Technical Report
Air Force Office of Scientific Research

DETECTABILITY MODELS AND WAVEFORM DESIGN FOR MULTIPLE ACCESS LOW PROBABILITY-OF-INTERCEPT NETWORKS

Glenn E. Prescott
Principal Investigator
Associate Professor of Electrical Engineering

Capt Robert F. Mills

October 1997

Telecommunications and Information Sciences Laboratory
Department of Electrical Engineering & Computer Science
University of Kansas, Lawrence, KS 66045

Abstract

Increased connectivity demands in the tactical battlefield have led to the development of multiple access low-probability-of-intercept (LPI) communication networks. Most detectability studies of LPI networks have focused on the individual network links, in which detectability calculations are carried out for a single network emitter. This report, however, presents a different approach to network detectability analysis: it is assumed that the interceptor does not attempt to distinguish one emitter from another, but rather decides only if a network is operating or not. What distinguishes this approach from conventional link intercept analysis is that detection decisions are based on energy received from multiple sources.

The following multiple access schemes are considered: frequency division, time division, direct sequence code division, and frequency hop code division. The wideband radiometer and its hybrids, such as the channelized radiometer, are used as potential network intercept receivers.

Two network detection models are developed. A dispersed network intercept model is appropriate for scenarios in which the network transmitters are dispersed throughout a fixed tactical region, and the interceptor is inside the network. The intercept area for the specified probabilities of detection and false alarm is used as a performance metric. A stand-off network intercept model is used for situations in which the network transmitters are collocated and the interceptor is standing-off. The performance metric for this model is a network LPI quality factor, which directly relates the network's operating range to the intercept range, as a function of the waveform parameters and the interceptor's desired performance level.

Covert signal design strategies applicable to LPI networks are then presented. Techniques for improving network covertness include modulation and coding, and data rate reduction using pulse combining. The effects of varying waveform parameters on the

performance of various intercept receivers are also investigated.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

An area of critical importance to military commanders is the vulnerability of their communication systems to interception and exploitation. While an anti-jamming capability is an essential feature for military communication systems, there are situations in which communications covertness is more important. For example, the requirement for covert operation of military aircraft has driven the design of stealth aircraft with small radar cross sections in an attempt to minimize the likelihood of detection by surveillance radars. Likewise, the reduction of communications detectability, resulting in a low-probability-of-intercept (LPI) communication system, is also critical to mission covertness. LPI principles are becoming progressively more important to the commercial sector as well. The features that render a waveform less detectable to unintended listeners also make it less likely the signal will interfere with other users. This offers the potential for developing communications networks capable of supporting more active users than when conventional multiple access techniques are used.

Generally, past LPI research has focused on the point-to-point communication link, consisting of a transmitter-receiver pair, one or more jammers, and an intercept receiver. A number of models have been developed to analyze the link's detectability. Typically, each device is identified by a set of operational parameters, such as power, signal bandwidth, required bit error probability, etc., and an overall detectability equation is developed using link budget analysis techniques. A common measure of how well the LPI link operates is the ratio of communication range to intercept range: that

is, for a given separation between the transmitter and receiver, how far away can the interceptor detect the signal?

The logical extension for the LPI communications link is to connect multiple users into a unified network. A multiple access LPI (MALPI) network is then defined as a collection of users sharing a radio frequency channel such that the detectability of the overall network is minimized. Although a number of studies ([0, 0], for example) have investigated the design issues for LPI networks, detectability analyses are typically carried out for a single network transmitter, rather than for the network at large. While this is a valid approach (effective LPI link design will inherently improve the covertness of the network), the impact of multiple transmitters has not really been addressed. Specifically, the following questions arise:

- What is meant by detection of a network, and how does it differ from that of a single link?

- What is the best type of intercept receiver for a given network structure?

- How does the detectability depend on the multiple access scheme?

- How can the network be designed and/or operated to minimize overall detectability?

1.2 Problem Description

The primary purpose of this research was to develop models for determining the detectability of MALPI networks, in which the interceptor does not attempt to isolate a particular transmitter. Based on these models, network LPI performance metrics were then developed to allow comparisons among various intercept strategies and network structures to provide insight into the design and analysis of LPI networks. Finally, waveform design techniques were developed for use in improving network covertness.

1.2.1 Scope

The following multiple access schemes were considered in this research: frequency division (FDMA), time division (TDMA), direct sequence code division (DS-CDMA),

and frequency hop code division (FH-CDMA). Intercept receivers include the wideband radiometer, channelized radiometer, and binary moving window type detectors, which exploit the discrete distribution of signal energy in the time-frequency space. The effects of jamming and interference were not considered.

1.2.2 Assumptions

To simplify the problem of analyzing a tactical network, the following assumptions were used:

- All network transmitters are confined to a limited geographic region. Users may be fixed or mobile; they may be on the ground, at sea, or in the air.

- The interceptor in general does not know the relative position of, nor direction to, the network users. The interceptor's goal is merely to determine if the network is in operation.

- The interceptor does know the fixed parameters of the network signal structure (i.e., chip rate, frequency hop rate, bandwidths, etc.), and has good estimates of the probability distributions of any pseudorandom parameters.

- Static networks are assumed—communication resources are assigned in a fixed assignment fashion; entry/withdrawal, message routing, and throughput issues are not considered.

- Free space $(1/R^2)$ propagation is used.

- Transmitter power levels remain fixed for the interceptor's observation time.

- Omnidirectional antennas are used within the network.

These assumptions are not overly restrictive, considering the tactical nature of the network, and they are consistent with previous research in this area [0, 0].

1.2.3 Summary of Current Knowledge

Most of the published work in the area of LPI communications is deals with the design and analysis of the point-to-point link, as discussed earlier. Much of the LPI research from the 1970s and 1980s is summarized in [0].

Waveform Analysis

In the mid-1970s there was considerable interest in the development of LPI communication systems, especially by the Naval Research Laboratory, which published several reports on LPI waveform design and detectability [0, 0, 0]. However, military planners decided that anti-jam protection was paramount, and LPI research received little attention until the late 1980s. More recently, researchers from the Avionics Laboratory at Wright-Patterson AFB have developed techniques for LPI communications system design on a single link basis (transmit power, modulation, antennas, etc.) using LPI *quality factors* [0]. Analysis tools based on these quality factors have been developed [0] and are now in use by several US research laboratories in evaluating the detectability of LPI waveforms against candidate intercept receiver structures.

Intercept Receivers

Most of the theory associated with intercept receivers and radiometric detectors was adapted from radar detection applications from nearly 30 years ago. Classic papers on noncoherent detection by Barton [0] and Urkowitz [0] have been used in the development of several radiometer detection models [0, 0, 0]. The purpose of these detection models is to provide a closed form relationship between the desired performance of the radiometer (specified by its probabilities of false alarm and detection) and the required signal-to-noise ratio at the receiver input. An in-depth analysis of the derivations of these models has shown them to be roughly equivalent for spread spectrum signals with large time-bandwidth products [0].

LPI Networks

As discussed previously, there have been a few efforts in the area of LPI network design, as well. Two efforts in particular have investigated the interaction between waveform parameters and signal detectability, although detectability calculations are limited to the interception of a single transmitter.

The *LPI Waveform Study* [0], produced for USAF Rome Laboratory, is a comprehensive technical report addressing a wide range of issues including general network design concepts (such as throughput requirements and topology), covert waveform design, and

artificial intelligence-based network control.

A similar effort was performed for the US Army Research Office in support of their distributed spread spectrum radio network research program [0]. The purpose of this research was to identify key parameters affecting operation of each network communication link (i.e., transmitter power, antenna gains, etc) and develop a strategy for controlling these parameters on a network-wide basis. Only direct sequence CDMA networks were considered.

1.3 Approach

This research consisted of three major tasks. First, network intercept models were developed to relate the performance of the intercept receiver (in terms of its probability of false alarm, probability of detection, and received signal-to-noise ratio) to the network's physical and waveform parameters. This included development of appropriate intercept strategies which exploit certain features of the network waveforms, such as frequency channelization or time division multiplexing. Since radiometric intercept receivers were used in this research, the detection models are based on the received energy from each network transmitter.

Second, performance metrics were derived to allow comparisons between different intercept strategies, and to evaluate the effects of varying signal parameters on the detectability of the network. An effective measure of any LPI system, be it a single link or a network of many users, is the expected region (as measured by range, area, or volume) of communications compared to the potential region of interception.

In the final task, waveform design techniques were developed to reduce network detectability. Performance comparisons between intercept receivers as a function of waveform parameters were also investigated, by applying the detectability models and performance metrics developed in the previous tasks.

1.4 Sequence of Presentation

This report consists of five chapters, including this introduction. Chapter 2 contains background information on LPI link analysis, fundamental intercept receivers, and multiple access network schemes. Key LPI topics include development of the *LPI Equation* and LPI quality factors which greatly simplify the analysis and design of LPI links. An overview of interception strategies and common intercept receivers, such as the wideband and channelized radiometers, is also presented. Finally, issues regarding the application of LPI techniques to multiple access networks are covered.

The topic of Chapter 3 is the detection of multiple access networks. First, the differences between link and network interception are explored. Then, network detectability models and LPI performance metrics are developed for each intercept receiver and multiple access scheme considered in this research. Examples illustrating the application of these models are also presented.

Waveform design techniques which are suitable for use in multiple access LPI networks are then presented in Chapter 4. Intercept receiver performance comparisons as a function of network waveform parameters, are also presented. Examples illustrating the use of these techniques are included. Chapter 5 provides a brief summary of this research, along with recommendations for further study.

Chapter 2

Fundamentals: LPI, Detection, and Networks

Before multiple access LPI networks can be discussed in any detail, it is desirable to review the fundamentals of LPI communication system design, signal interception, and multiple access networks. In this chapter, the following topics are covered:

- Analysis of the typical point-to-point LPI communications link

- LPI system quality factors and how they are employed to simplify the design and analysis of an LPI communication link

- Common LPI waveforms

- Radiometric detection techniques and strategies

- Application of LPI techniques to multiple access networks

2.1 Typical Intercept Scenario

Figure 2.1 depicts a typical point-to-point LPI link scenario, in which a cooperative transmitter and receiver are targeted by jammers, which disrupt the communications receiver, and intercept receivers, which attempt to detect and exploit the transmitted signal.

The objective of any LPI communication system is to conduct information between a transmitter and receiver while minimizing the ability of an unauthorized listener to intercept, classify, or otherwise exploit the transmitted signal. The communication
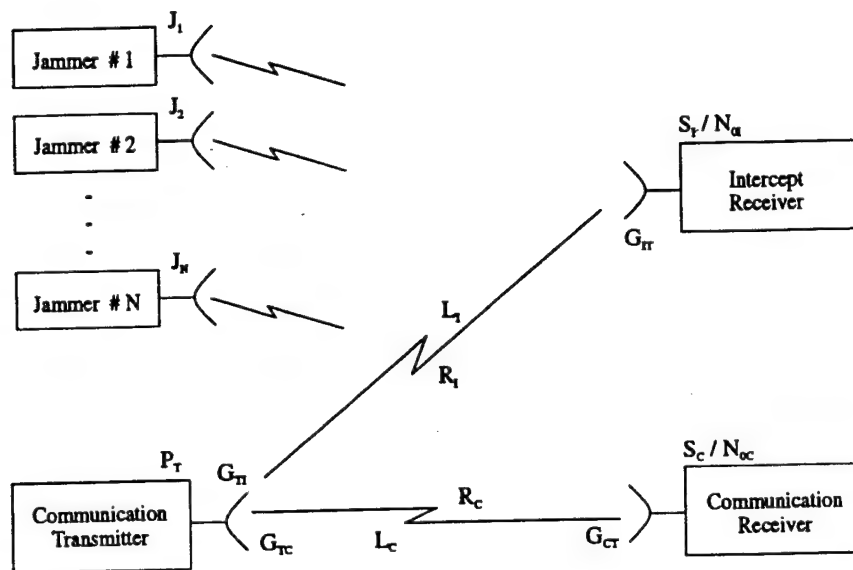
Figure 2.1: Typical LPI Scenario

system has a variety of techniques for reducing the probability of intercept: steerable high gain antennas, adaptive transmitter power control, and transmitted waveforms with large time-bandwidth products and noise-like spectra, just to name a few. Likewise, the interceptor has similar technologies, such as directional, low sidelobe antennas and adaptive filtering.

2.1.1 LPI Communication Link Analysis

The communication system is characterized by several performance parameters which are evaluated to determine how well the system performs. For example, the transmitter is characterized by its power, antenna gain, and modulation type, while the receiver is characterized by its antenna gain, noise bandwidth, and system temperature. There is always some performance requirement imposed on a communication system, usually specified as the bit error probability, P_E, which then determines the required signal-to-noise ratio (SNR) for the given modulation scheme:

$$\frac{S_C}{N_{SC}} = R_b \frac{E_b}{N_{SC}} \tag{2.1}$$

where

- S_C is the received signal power

- N_{SC} is the power spectral density (PSD) of the noise and interference at the input to the receiver

- R_b is the communication data rate (bits per second)

- E_b/N_{SC} is the bit energy to noise PSD required to achieve the desired P_E

The noise/interference PSD, N_{SC}, is the sum of PSDs due to additive white Gaussian noise (AWGN), N_{0C}, and interference/jamming, N_{JC}:

$$N_{SC} = N_{0C} + N_{JC} \tag{2.2}$$

where

$$N_{0C} = kT_{aC} + kT_0(F_C - 1) \tag{2.3}$$

$$N_{JC} = \sum_{n=1}^{N} \sum_{m=1}^{M} g_{Cn} g_{Cm} \frac{J_{mnC}}{B_C} \tag{2.4}$$

and

- k is Boltzmann's constant

- B_C is the noise bandwidth of the communications receiver

- T_{aC} is the communications antenna noise temperature

- T_0 is the room temperature (290° K)

- F_C is the communications receiver noise figure

- J_{nmC} is the jamming component from the nth jammer at the mth frequency component

The jamming PSD accounts for the effect of N jammers, which are assumed to transmit in discrete frequency cells. J_{nmC} represents the power level transmitted by the nth jammer (out of N total) in the mth frequency slot (M total). The factors g_{Cn} and g_{Cm} represent the null-steering and interference suppression factors, respectively, which act

together to reduce the effect of J_{nmC}. In a dense jamming environment, N_{SC} will be dominated by the jamming ($N_{SC} \approx N_{JC}$), while in a jam-free environment, thermal noise dominates ($N_{SC} \approx N_{0C}$).

Using link budget techniques, the received signal power at the receiver is

$$S_C = \frac{P_T G_{TC} G_{CT}}{(4\pi R_C/\lambda)^2 L_C} \qquad (2.5)$$

where

- P_T is the transmitter power

- G_{TC} is the transmitter antenna gain in the direction of the receiver

- G_{CT} is the receiver antenna gain in the direction of the transmitter

- R_C is the distance between the transmitter and receiver

- $(4\pi R_C/\lambda)^2$ is the propagation loss (assuming free space $1/R^2$ propagation)

- λ is the transmission wavelength ($\lambda = c/f$)

- L_C is the atmospheric loss factor, which accounts for losses due to rain and water vapor

Using (2.1) and (2.5), the received signal power to noise PSD can be expressed in terms of the link parameters:

$$\frac{S_C}{N_{SC}} = R_b \frac{E_b}{N_{SC}} = \frac{P_T G_{TC} G_{CT}}{L_C N_{SC}} \left(\frac{\lambda}{4\pi R_C}\right)^2 \qquad (2.6)$$

Solving for the communication range R_C yields

$$R_C = \sqrt{\frac{P_T G_{TC} G_{CT}}{L_C N_{SC}} \left(\frac{\lambda}{4\pi}\right)^2 \frac{1}{S_C/N_{SC}}} \qquad (2.7)$$

2.1.2   Intercept Link Analysis

Analysis of the intercept link proceeds in a similar fashion. The available signal power at the intercept receiver is

$$S_I = \frac{P_T G_{TI} G_{IT}}{(4\pi R_I/\lambda)^2 L_I} \qquad (2.8)$$

where

- G_{TI} is the transmitter antenna gain in the direction of the receiver

- G_{IT} is the receiver antenna gain in the direction of the transmitter

- R_I is the intercept range

- L_I is the atmospheric loss in the intercept link

Solving for the intercept range gives

$$R_I = \sqrt{\frac{P_T G_{TI} G_{IT}}{L_I N_{SI}} \left(\frac{\lambda}{4\pi}\right)^2 \frac{1}{S_I/N_{SI}}}$$
(2.9)

where N_{SI} is the noise/interference PSD:

$$N_{SI} = N_{0I} + N_{JI}$$
(2.10)

with

$$N_{0I} = kT_{aI} + kT_0(F_I - 1)$$
(2.11)

$$N_{JI} = \sum_{n=1}^{N} \sum_{m=1}^{M} g_{In} g_{Im} \frac{J_{mnI}}{B_I}$$
(2.12)

and

- B_I is the noise bandwidth of the intercept receiver

- T_{aI} is the intercept antenna noise temperature

- T_0 is the room temperature (290° K)

- F_I is the intercept receiver noise figure

- J_{nmI} is the jamming power level from the nth jammer at the mth frequency component

- g_{In} and g_{Im} are the null-steering and interference suppression factors for the nth jammer and mth frequency tone, respectively

The received signal power to noise PSD ratio, S_I/N_{SI}, determines the achievable performance of the interceptor, as described by its probability of detection, P_D, and probability of false alarm, P_F. For any desired P_D and P_F, there is some required S_I/N_{SI}, which then determines the maximum intercept range, given in (2.9). Beyond this range, the interceptor will not achieve its performance requirements.

2.1.3 LPI Quality Factors

In the previous sections, expressions for the communication and interception ranges were derived in terms of the scenario parameters (antenna gains, losses, etc.) and the desired performance: P_E for the communication receiver; P_D and P_F for the intercept receiver. The purpose of LPI is to maximize R_C with respect to R_I, as shown below:

$$\left(\frac{R_C}{R_I}\right)^2 = \frac{G_{CT}G_{TC}}{G_{IT}G_{TI}} \frac{L_I}{L_C} \frac{N_{SI}}{N_{SC}} \frac{S_I/N_{SI}}{S_C/N_{SC}} \tag{2.13}$$

Equation (2.13) is commonly referred to as the *LPI Equation*. There are many options for increasing R_C/R_I, such as reducing G_{TI} (using low sidelobe antennas) or reducing the required S_C/N_{SC} (through modulation and coding), which make the LPI link more difficult to detect. The objective is to make the intercept receiver move unacceptably close to the transmitter (thus increasing its physical risk) in order to achieve its performance requirements.

LPI quality factors can be used to facilitate the analysis of various tradeoffs in (2.13). These quality factors are quite useful since they allow a direct comparison of the performance requirements of the two receivers. Furthermore, parameters which are common to both of the links (such as P_T and λ) are not considered.

LPI Quality Factor

The *LPI quality factor* is defined in decibels as

$$Q_{LPI} = 20 \log\left(\frac{R_C}{R_I}\right) \tag{2.14}$$

As indicated by this expression, any action which improves the covertness of the communication link will either allow the communication system to operate over a longer range or force the interceptor to move closer to the transmitter to achieve its desired performance level. Q_{LPI} is increased by designing LPI features into the system such that the

terms in (2.13) are maximized. In fact, each of these terms can also be expressed as a quality factor:

$$Q_{LPI} = Q_{ANT} + Q_{ATM} + Q_{IS} + Q_{MOD} \qquad (2.15)$$

where

- Q_{ANT} is the *antenna* quality factor

- Q_{ATM} is the *atmospheric* quality factor

- Q_{IS} is the *interference suppression* quality factor

- Q_{MOD} is the *modulation* quality factor

Each of these quality factors is discussed in the following sections.

Antenna Quality Factor

The antenna quality factor is defined as

$$Q_{ANT} = 10\log\left(\frac{G_{CT}G_{TC}}{G_{IT}G_{TI}}\right) \qquad (2.16)$$

Q_{ANT} accounts for any advantages provided by using high quality antennas. To maximize Q_{ANT}, the communicator designs G_{CT} and G_{TC} to be large and G_{TI} to be small—steerable, high-gain antennas with low sidelobes are generally used.

The communicator has no control over the interceptor antenna gain, G_{IT}. If G_{IT} is large, Q_{ANT} will be reduced. The interceptor cannot arbitrarily increase G_{TI}, however, since a smaller beamwidth requires a longer search time to acquire the LPI signal. The probability of missing a short transmitted pulse therefore increases when high-gain antennas are used by the interceptor.

Atmospheric Quality Factor

The atmospheric quality factor, Q_{ATM}, accounts for the relative atmospheric effects in the communication and intercept links. It is defined in decibels as

$$Q_{ATM} = \xi_I R_I - \xi_C R_C \qquad (2.17)$$

where ξ_I and ξ_C are loss factors, expressed in dB/km or dB/mile. In most cases, the path losses in the communication and intercept links can be assumed to be equal (excluding the free space loss), since the interceptor and communications receiver are close together and operate in essentially the same atmospheric conditions.

Interference Suppression Quality Factor

The interference suppression quality factor compares the ability of the intercept and communications receiver to suppress or minimize interference. Q_{IS} is defined as follows,

$$Q_{IS} = 10 \log \left(\frac{N_{SI}}{N_{SC}} \right) \tag{2.18}$$

Using Equations (2.2) and (2.10) with (2.18) yields

$$Q_{IS} = 10 \log \left(\frac{kT_{aI} + kT_0(F_I - 1) + \sum_{n=1}^{N} \sum_{m=1}^{M} g_{In} g_{Im} \frac{J_{mnI}}{B_I}}{kT_{aC} + kT_0(F_C - 1) + \sum_{n=1}^{N} \sum_{m=1}^{M} g_{Cn} g_{Cm} \frac{J_{mnC}}{B_C}} \right) \tag{2.19}$$

If the two receivers effectively eliminate any jamming interference, Q_{IS} is dominated by the respective noise figures and antenna temperatures. Usually, the interference suppression filters are adaptive excision filters, and are intended to whiten the interference environment. The ability of either receiver to null out interference from a particular frequency cell or jammer will increase or decrease Q_{IS} accordingly.

Modulation Quality Factor

The modulation quality factor is probably the most significant quality factor, since it allows a direct performance comparison for the two receivers. Q_{MOD} is defined in decibels as

$$Q_{MOD} = 10 \log \left(\frac{S_I/N_{SI}}{S_C/N_{SC}} \right) \tag{2.20}$$

Q_{MOD} ignores all *scenario dependent* factors, which are accounted for by Q_{ANT}, Q_{ATM}, and Q_{IS}—only the parameters of the signal (modulation, bandwidth) and the detection method (noncoherent, coherent) are important. Any action which increases the required SNR at the intercept receiver or decreases the required SNR at the communication receiver increases Q_{MOD}.

The relative performance of the two receivers is paramount. Although the communication receiver has *a priori* knowledge of the signal structure, the interceptor makes

decisions regarding only the presence or absence of the signal and not the actual content. Hence the interceptor often requires less SNR to meet its performance requirements.

The required SNRs for both receivers can be expressed as functions of performance and signal parameters. The intercept SNR depends on the desired P_D and P_F, the observation time, T, and intercept bandwidth, W. Likewise, the communication receiver's SNR depends on the desired P_E, modulation, and data rate. Thus, Q_{MOD} can be expressed as

$$Q_{MOD} = \frac{\zeta_I(P_D, P_F, T, W)}{\zeta_C(P_E)R_b} \tag{2.21}$$

To use (2.21), appropriate expressions for $\zeta_C(P_E)$ and $\zeta_I(P_E, P_F, T, W)$ are required. The value of $\zeta_C = E_b/N_0$ can be obtained from digital modulation performance curves, or from analytic representations, such as those given in Table 2.1. ζ_I depends on the type of intercept receiver being used and the detection parameters. Several intercept receiver models have been developed and are presented in [0, 0]. Development of a detection model for the wideband radiometer is discussed in Section 2.3.

Modulation Type	$\zeta_C(P_E) = E_b/N_0$
Noncoherent Binary FSK	$-2\ln(2P_E)$
Differentially Coherent BFSK	$-\ln(2P_E)$
Coherent BPSK/QPSK	$\left[Q^{-1}(P_E)\right]^2/2$

Table 2.1: Required E_b/N_0 as a Function of Desired P_E

Interpretations and Use of Quality Factors

LPI system quality factors are extremely useful in designing an LPI system, because the various tradeoffs involved can be quickly assimilated. In (2.14), there are several factors which can be directly controlled by the LPI system designer. First, high-gain antennas with low sidelobes can be used to maximize Q_{ANT}. Second, interference-excision filters can be used to reduce the effect of jammers and thus maximize Q_{IS}. Finally, effective LPI waveforms can be used to maximize Q_{MOD}. Any LPI improvement can then be used several ways:

1. Operate the LPI link over a longer range, with all other parameters remaining constant.

2. Reduce transmit power (keeping R_C constant), which reduces the intercept range

3. Maintain constant R_C and R_I, and trade the increase for a decrease elsewhere in the system design (i.e., trade an improvement due to modulation and coding for cheaper antennas)

2.2 Common LPI Waveforms

As discussed in the previous section, the covertness of an LPI communication link can be improved by increasing the modulation quality factor. This is accomplished by using waveforms which are inherently more difficult to detect or intercept. There are many classes of waveforms which can be used for LPI purposes, ranging from simple structures to complex hybrids, and providing different LPI capabilities. These waveforms often exhibit antijam (AJ) properties as well.

2.2.1 Direct Sequence

Direct sequence (DS) spread spectrum modulation is equivalent to BPSK or QPSK modulation, except a high bit rate pseudorandom binary waveform is combined with the information data stream before modulating the carrier. The result is a waveform having a spectrum many times wider than if just data were used to modulate the carrier. Furthermore, the power spectral density of the waveform is reduced considerably, and is often indistinguishable from background noise.

The communication receiver knows the spreading code used at the transmitter and can despread the signal, in effect yielding a narrowband system. LPI is achieved because the interceptor does not know the spreading code and must therefore use a wideband receiver to capture all of the transmitted energy, thus accepting more noise as well. AJ capability is obtained, because any jamming signals are spread at the communication receiver during the despreading process.

The bandwidth expansion factor is roughly the ratio of the chip rate of the pseudorandom bit stream to the bit rate of the information data. This ratio is generally

defined as the processing gain:

$$PG = \frac{R_c}{R_b} \approx \frac{W_1}{W_{data}} \qquad (2.22)$$

The energy distribution for the DS waveform is shown in Figure 2.2. Because of the spreading, $T_1 W_1 \gg 1$.
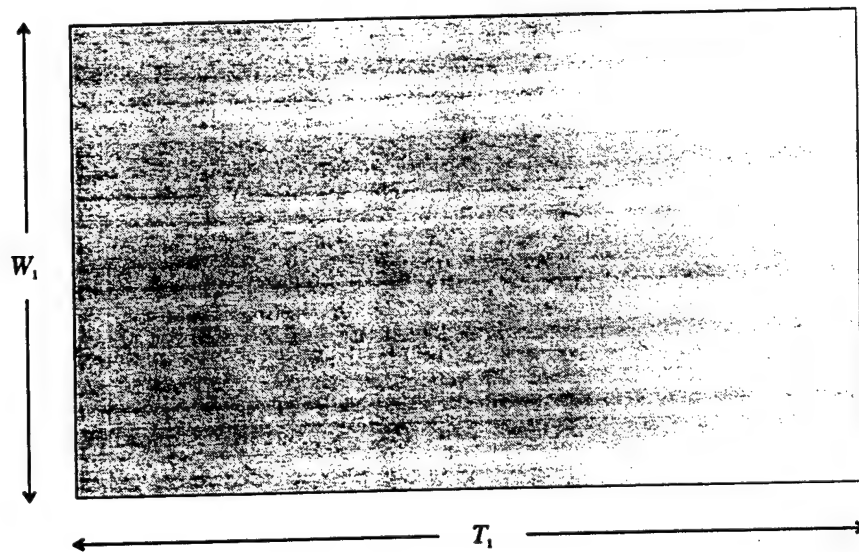
Figure 2.2: Time-Frequency Diagram for a DS BPSK Signal

2.2.2   Frequency Hopping

Figure 2.3 shows the energy distribution for a frequency hopping (FH) signal, in which the carrier frequency changes according to a pseudorandom pattern. The total bandwidth and message duration time are W_1 and T_1, respectively, while the bandwidth and duration of each hop are W_2 and T_2. The hop rate is $R_h = 1/T_2$, and there are M frequency channels (not necessarily contiguous) and N hops in the total message time. LPI (and AJ) capability is achieved since the interceptor (or jammer) does not know the exact hop sequence.

In a *slow* FH system, the hop dwell time is greater than the data symbol duration (i.e., multiple symbols per hop), and $T_2 W_2 > 1$. In a *fast* FH system, the hop dwell time
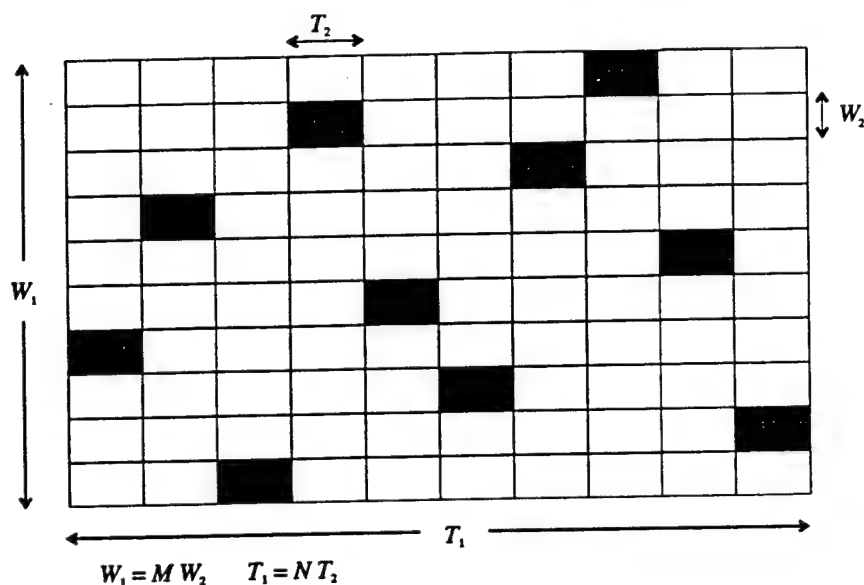
Figure 2.3: Time-Frequency Diagram for a Frequency-Hopped Signal

is shorter than the symbol duration (multiple hops per symbol), and $W_2 \approx R_h = 1/T_2$. Pulsed FH signals can be generated by using a duty cycle less than 100 percent. While there are no LPI benefits to this modification, AJ performance can be improved. With pulsed FH, $W_2 T_2 \approx 1$, but $W_2 > R_h$. The duty cycle is $\alpha = N T_h / T_m$.

2.2.3 Time-Hopping

Figure 2.4 shows the energy distribution for a typical time-hopping (TH) signal, in which the transmission time slots are selected according to a pseudorandom pattern. During each frame time, T_F, a new time slot of duration T_2 is selected; the entire bandwidth W_1 is available to each user. LPI benefits arise because the time uncertainty forces the interceptor to use a longer observation interval than the signal's duration; hence noise-only samples are added to the detection process. Likewise, AJ is improved because the jammer must match its transmission time to that of the communication transmitter.

2.2.4 Hybrid Waveforms

LPI and AJ performance can be improved by combining various modulation schemes. Figure 2.5 illustrates the FH/TH hybrid, in which the time slots and frequency channels are both selected pseudorandomly. DS modulation could also be used within each pulse.
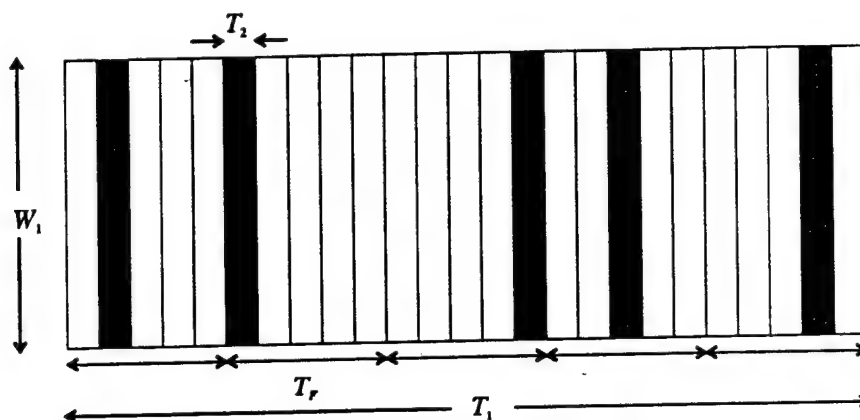
Figure 2.4: Time-Frequency Diagram for Time-Hopped Signal
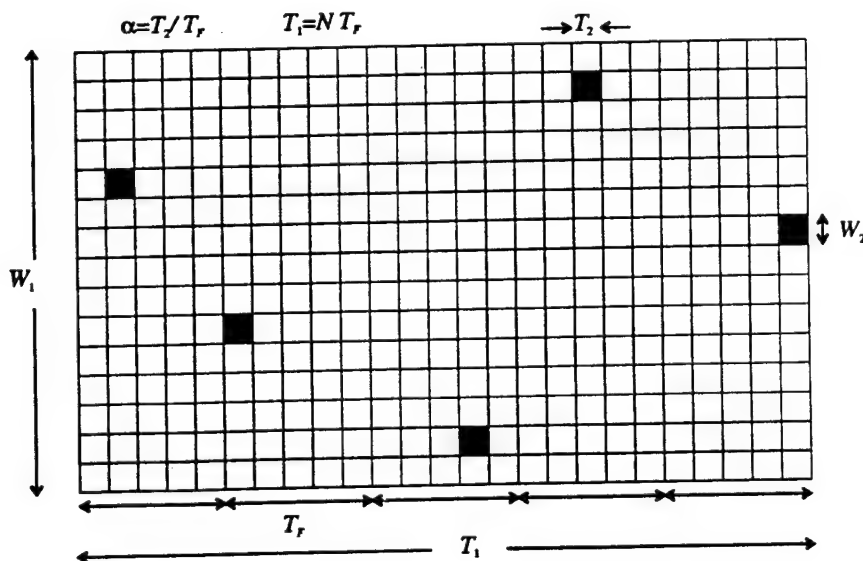
Figure 2.5: Time-Frequency Diagram for FH/TH Signal

2.2.5 LPI versus Antijam

The characteristics of antijam (AJ) and LPI links are in many cases similar. These similarities are due to the waveforms used rather than design philosophy. For an effective AJ capability, a communication link is designed such that a large signal-to-noise ratio and plenty of excess margin is available at the receiver. Spread spectrum waveforms, such as FH and DS are used to provide processing gain.

Spread spectrum waveforms are also used in LPI links because they provide large bandwidths and low-level power densities. However, unlike AJ systems, LPI systems are designed such that the absolute minimum SNR required to provide the minimum level of acceptable performance is available at the receiver. As discussed in Section 2.1, every factor in the link equation is carefully considered (transmitter power, antenna gains, range, etc.) such that the link operates at the desired performance level. Excess power levels are avoided because they increase the detectability of the system.

AJ and LPI systems also differ in their perceived threats and survivability require- ments. The threat to an AJ system is that a jammer may be able to disrupt the receiver and therefore deny the use of that data link for tactical purposes. This would result in varying degrees of mission impairment, depending on the purpose of the communica- tion link. At one extreme, the denial of a communication channel may force the user to select a different frequency, which is free of jamming. At the other extreme, a weapons platform may fail to release its weapon, miss the desired target, or perhaps even hit an unintended target, causing a large amount of collateral damage.

The threat to an LPI system is that hostile forces will be able to detect covert trans- missions and then possibly intercept and exploit the information (see [0] for a complete discussion of these concepts). Again there are varying degrees of mission impairment, such as a compromise of information regarding troop movements, or detection and cap- ture of a covert search and rescue mission.

Because jamming is an *active* process, the users of a jammed communication link will know when the link fails due to jamming. Corrective measures, such as the use of alternate frequencies, can then be implemented, and mission impairment may be minimized. In contrast, interception is a *passive* process, and the LPI communicator will generally not know if the signal has been intercepted. Hence, *any* detection or interception of a covert message could could conceivably result in mission failure.

In summary, the similarities between AJ and LPI communication links end at the waveform selection process. AJ systems make no attempt to hide their signal, and operate with the premise that jammers will attempt to disrupt the signal—power and processing gain are used to overcome any interference. Covertness, on the other hand, is the key to LPI communications. Although LPI communication links exhibit some AJ properties, their true strength lies in concealment.

2.3   Basic Detection Techniques

In this section, several fundamental techniques for detecting spread-spectrum LPI signals are discussed. Topics include some of the more common intercept receivers, such as the wideband radiometer, and how they can be used to detect the various spread-spectrum waveforms discussed in the previous section.

2.3.1   Detection Strategy

The ability to detect or intercept a spread-spectrum signal depends a great deal on how much the interceptor knows about the signal (i.e., carrier frequency, hop rate, pulse timing, etc.). In [0], five levels of interceptor knowledge are defined. At level one, the interceptor knows nothing about the signal, while level five assumes the interceptor has complete knowledge. Neither extreme is realistic, and it is generally assumed that the interceptor knows the fixed parameters of the signal and has estimates of the probability distributions of any pseudorandom parameters. This constitutes a "worst case" scenario (from the LPI communicator's perspective), in which the interceptor designs and builds the best possible receiver [0].

Dillard and Dillard ([0, 0]) give a useful detection model, illustrated in Figure 2.6 which can be applied to a variety of scenarios. The model has two main elements. The *coarse* structure defines how the data symbols are distributed in time and frequency in the total system time-bandwidth plane. The *micro* structure defines the energy distribution within each data symbol; the two types of micro structures include pseudonoise (PN) and frequency hop (FH). The individual parameters of the detection model are described in Table 2.2 (from [0]).

The interceptor does not know enough about the transmitted signal to use coherent processing techniques, so noncoherent detection methods are usually used. Most intercept receivers use square-law devices followed by a filter or integrator to detect energy or signal features, such as the hop rate or chip rate. There has been a great deal of research lately on detectors which exploit spectral correlation, such as the single cycle detector [0]. Radiometric receivers are used exclusively in this research.
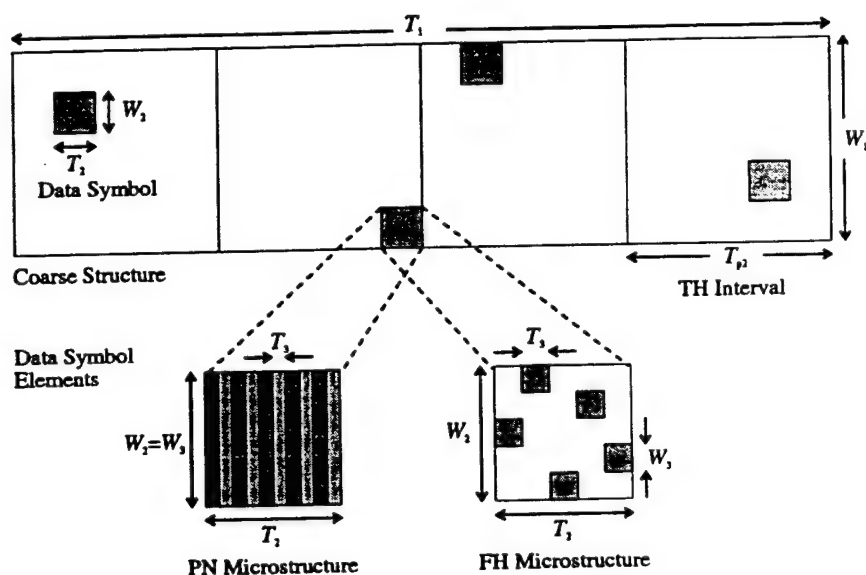
Figure 2.6: Generic Spread-Spectrum Waveform Detection Model

Signal Structure Categories	Notation	Definition
All Categories	T_1, W_1	Duration and bandwidth of transmission
	E_1	Signal energy of transmission
Data symbols each contain a number of signaling elements; i.e., the symbol has an FH, TH, or PN structure. If the structure is PN, the value of T_3 usually can be disregarded in detectability calculations.	T_2, W_2	Duration and bandwidth of data symbol
	b_2	Number of data symbols per transmission
	T_{p2}	Duration of hop interval $(T_{p2} = T_1/b_2)$
	E_2	Signal energy in data symbol
	T_3, W_3	Duration and bandwidth of elements $(T_3 W_3 \approx 1)$
	b_3	Number of elements per data symbol
	T_{p3}	Duration of hop interval $(T_{p3} = T_2/b_3)$
	E_3	Signal energy of element
Data symbols each have only one signaling element	T_2, W_2	Duration and bandwidth of data symbol $(T_2 W_2 \approx 1)$
	b_2	Number of data symbols per transmission
	T_{p2}	Duration of hop interval
	E_2	Signal energy of data symbol

Table 2.2: Definitions for Dillard's Signal Detectability Model

2.3.2 Wideband Radiometer

The simplest intercept receiver is the *wideband* or *total power* radiometer, shown in Figure 2.7. The radiometer estimates the energy received in a given bandwidth, W, over the observation interval, T. Normally, T and W are matched to those of the signal so as to capture all available energy, without integrating noise-only samples. However, sometimes it is beneficial to restrict the bandwidth slightly, or to weight the frequency components as discussed in [0].
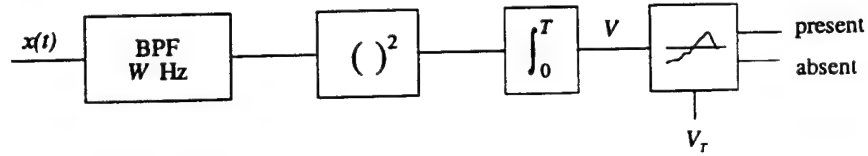
Figure 2.7: Radiometer Block Diagram

The test statistic V is formed by bandpass filtering the input signal, squaring, and then integrating. If the random variable V exceeds the detection threshold V_T, a signal is assumed to be present. If not, the signal is assumed to be absent. It can be shown that when the input to the radiometer is strictly AWGN, the normalized test statistic, $2V/N_0$, has a chi-square probability density function (pdf) with $2TW$ degrees of freedom. If a signal is present, $2V/N_0$ has a noncentral chi-square pdf with $2TW$ degrees of freedom and noncentrality parameter $2E/N_0$, where E is the energy of the signal measured over T seconds. Sample pdfs for the two hypotheses are depicted in Figure 2.8.

For the normalized decision threshold, $2V_T/N_0$, the probability of detection, P_D, and probability of false alarm, P_F, are determined as follows:

$$P_D = \int_{2V_T/N_0}^{\infty} p_{sn}(y) \, dy \qquad (2.23)$$

$$P_F = \int_{2V_T/N_0}^{\infty} p_n(y) \, dy \qquad (2.24)$$

where $p_n(y)$ and $p_{sn}(y)$ are the noise-only and signal plus noise density functions, respectively.

The performance of the radiometer is completely specified by $2E/N_0$, P_D, and P_F. Generally, P_D and P_F are specified according to mission objectives, and the required
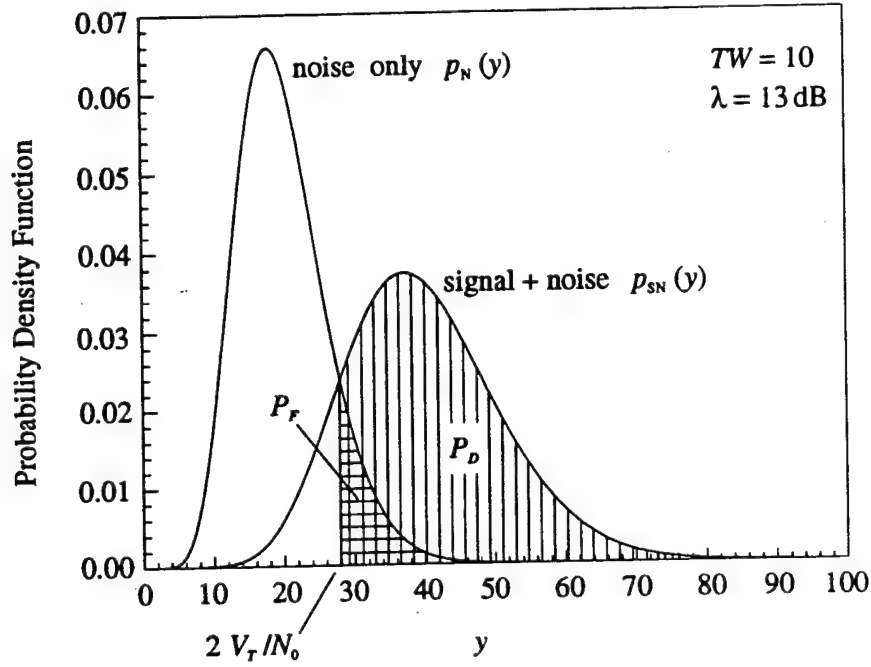
Figure 2.8: Chi-square Density Functions for Radiometer Test Statistic

SNR is then determined. Unfortunately, Equations (2.23) and (2.24) are not solvable in closed form, so a number of detectability models have been developed to provide the desired link between required SNR and desired performance. Several of these models are derived and compared in [0], and the models are typically accurate to within 0.5 dB for large time-bandwidth products ($TW > 1000$). Engler's model [0] is given as

$$\left(\frac{S_I}{N_0}\right)_{req} = \xi(P_D, P_F, T, W) = \frac{X_0 + \sqrt{X_0^2 + 16TWX_0}}{4T} \qquad (2.25)$$

where

$$X_0 = \left(Q^{-1}(P_F) - Q^{-1}(P_D)\right)^2 \qquad (2.26)$$

and $Q(x)$ is the tail integral of the zero-mean, unit-variance Gaussian density function:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-z^2/2} dz \qquad (2.27)$$

The results from (2.25) can be used directly in the modulation quality factor equation given in (2.21)). Engler's model is accurate to within 0.5 dB for $TW < 100$, with the

error approaching 0 dB for $TW > 1000$). A somewhat simpler model has been proposed by Edell [0]:

$$\left(\frac{S_I}{N_0}\right)_{req} = d\sqrt{\frac{W}{T}} \tag{2.28}$$

where $d = \sqrt{X_0} = Q^{-1}(P_F) - Q^{-1}(P_D)$. This model is accurate to within 0.3 dB for $TW \approx 1000$, with the error tending toward 0 dB as TW increases [0].

2.3.3 Pulse Detectors

When detecting frequency-hopped or pulsed signals, the interceptor can do either of the following: (1) employ a single wideband radiometer matched to the total spread spectrum bandwidth and integrate over the message duration, or (2) use radiometers matched to the duration and bandwidth of the individual pulses, and then form an overall detection decision. Generally, the second method is superior because the time-bandwidth product of the pulses is much smaller than the overall time-bandwidth product of the message, and noise has less effect on the detection process.

A class of detectors which are effective against signals consisting of distinct pulses (TH, FH) are *binary moving window* (BMW) detectors, shown in Figure 2.9. The detector forms a soft decision (designated as "0" or "1") after each pulse. If a sufficient number of pulses have been detected, an overall detection is declared. This process is also known in the literature under the following names [0]: binary integration, "k-out-of-b" detection, double threshold detection, and coincidence detection.
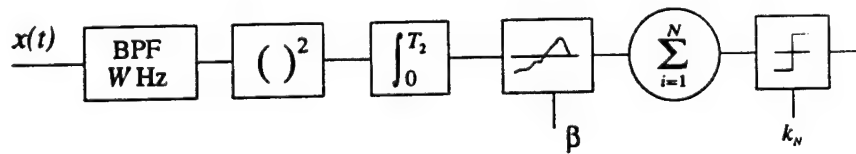
Figure 2.9: Binary Moving Window Detector

As an alternative to keeping a running sum, the contents of the binary accumulator can be reset after every N pulses. The performance of the integrate and dump detector is slightly easier to analyze. It is assumed that the radiometer's bandwidth and integration time are equal to those of the input signal pulses. It is also assumed that the

noise samples in each time slot are uncorrelated, so the pulse decisions are statistically independent.

The overall false alarm probability is the probability that k_N or more pulse decisions result in detections when in fact no signal is present. If Q_F is the probability of false alarm for a particular time slot, the probability of having exactly i out of N false alarms is $\binom{N}{i} Q_F^i (1 - Q_F)^{N-i}$, hence the overall probability of false alarm is

$$P_F = \sum_{i=k_N}^{N} \binom{N}{i} Q_F^i (1 - Q_F)^{N-i} \tag{2.29}$$

Similarly, the overall probability of detection is the probability that k_N or more pulse decisions result in detections when the signal is present—it is assumed that the signal is present during the entire observation interval. If Q_D is the single pulse detection probability, then the overall probability of detection is

$$P_D = \sum_{i=k_N}^{N} \binom{N}{i} Q_D^i (1 - Q_D)^{N-i} \tag{2.30}$$

To achieve specific probabilities of detection and false alarm, the allowable single pulse Q_F and Q_D are determined from (2.29) and (2.30). A suitable radiometer detection model (such as (2.28) or (2.25) can then be applied using T_2, W_1, and $X_0 = [(Q^{-1}(Q_F) - Q^{-1}(Q_D)]]^2$ to determine the required S_I/N_{0I}.

2.3.4 Channelized Radiometer

Likewise, if the interceptor knows the signal falls within a particular bandwidth during certain intervals, then a *channelized radiometer*, or *filter bank combiner*, shown in Figure 2.10 is an effective receiver. Such a detector is generally superior to the single wideband radiometer, because of the reduced receiver noise bandwidth.

Each channel consists of a separate radiometer with bandwidth W_2 and integration time T_2, which coincide with the signal's pulse structure. The number of hops observed is $N = T_1/T_2$, and if the channels are contiguous, $M = W_1/W_2$. [1] After each hop dwell time, the channel decisions are ORed to form the hop decision, which is then stored for the overall detection decision. To simplify the detector's performance analysis, it is

---

[1] Ideally, the number of channels should be matched to the number of frequencies in the hopset, but fewer channels can often be used (for economic and practical reasons) with adequate results [0, 0]
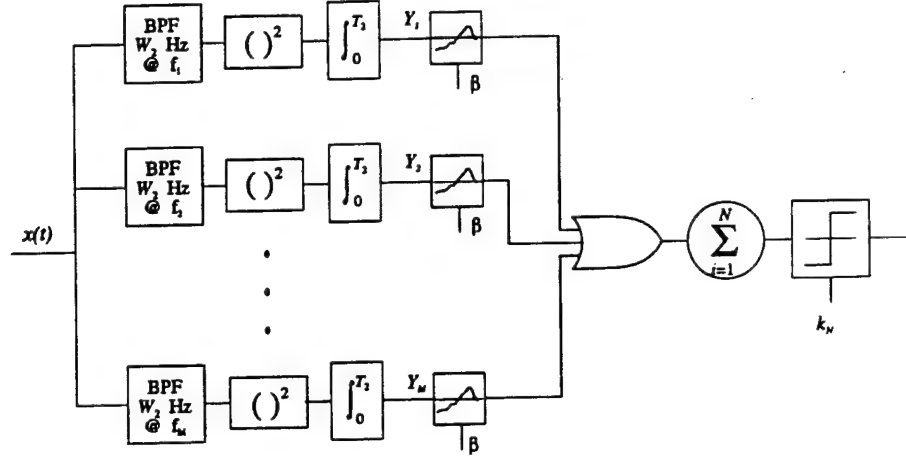
Figure 2.10: Channelized Radiometer (Filter Bank Combiner)

assumed that the noise samples in the channels are statistically independent (because their bandwidths are disjoint), and the hop decisions are independent.

The overall false alarm probability is the probability that k_N or more hop decisions result in a detection when no signal is present. If Q_F is the channel probability of false alarm, then the probability that none of the channels has a false alarm is $(1 - Q_F)^M$. Hence, the probability of a "1" at the output of the OR gate is

$$p_0 = 1 - (1 - Q_F)^M \tag{2.31}$$

The probability that this occurs exactly i out of the N hops is $\binom{N}{i} p_0^i (1 - p_0)^{N-i}$, so the overall probability of false alarm is

$$P_F = \sum_{i=k_N}^{N} \binom{N}{i} p_0^i (1 - p_0)^{N-i} \tag{2.32}$$

The overall probability of detection P_D is found in a similar manner. If Q_D is probability of detection for a channel containing signal energy, then the probability of a "1" at the output of the OR gate is simply the probability of a single missed detection and $M - 1$ correct nondetections:

$$
\begin{aligned}
p_1 &= 1 - \text{Prob[single miss and } M - 1 \text{ nondetections]} \\
&= 1 - (1 - Q_D)(1 - Q_F)^{M-1} \tag{2.33}
\end{aligned}
$$

The overall probability of detection is therefore

$$P_D = \sum_{i=k_N}^{N} \binom{N}{i} p_1^i (1 - p_1)^{N-i} \tag{2.34}$$

Given the desired P_D and P_F, p_0 and p_1 are solved using (2.32) and (2.34). The single channel probabilities Q_F and Q_D can then be determined as follows:

$$Q_F = 1 - (1 - p_0)^{1/M} \tag{2.35}$$

$$Q_D = 1 - \frac{1 - p_1}{(1 - Q_F)^{M-1}} \tag{2.36}$$

Once Q_F and Q_D have been determined, the required input SNR can be established using (2.25) or (2.28), using W_2, T_2, and $X_0 = d^2 = [Q^{-1}(Q_F) - Q^{-1}(Q_D)]^2$.

2.3.5 Other Detection Schemes

There are many other pulse detection schemes, each applicable to a particular waveform structure. Calculation of system performance for the detectors proceeds similarly to that presented in the previous sections. In summary, the following approach is used for LPI signal detectability analysis:

1. Obtain the overall performance (P_D and P_F) of the detector. This is usually dictated by mission requirements.

2. Work backwards using fundamentals of probability theory to determine the required performance levels at intermediate (soft decision) points (i.e., p_0 and p_1).

    — Solve inverse relationships of any summation operations

    — Solve inverse relationships for OR operations

3. Determine the performance requirements (Q_D and Q_F) for the radiometers matched to the individual FH/TH/PN pulses.

4. Use an appropriate radiometer detectability model to determine the required S_I/N_{0I} to achieve the appropriate Q_F and Q_D.

2.4   Application of LPI to Multiple Access Networks

The logical extension of the LPI link is the multiple access network, as shown in Figure 2.11. For the purposes of this research, a multiple access LPI network is defined as a multi-user network which has been specifically designed to operate in a tactical environment with minimized likelihood of detection, interception, and exploitation of network signals by unintended listeners. Users may be groundbased (fixed or mobile), maritime mobile, and airborne. As shown in the figure, the network may include smaller nets, such as a attack groups, which have their own specific communication requirements.
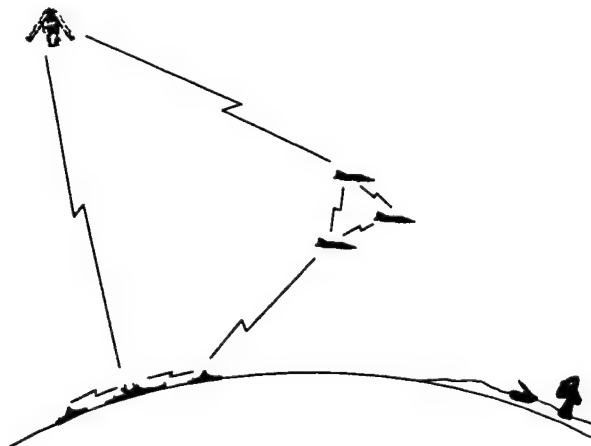
Figure 2.11: Typical Multiple Access LPI (MALPI) Network

As in the case of link design, the requirements and threats for AJ and LPI networks are fundamentally different. The threat to an AJ network is that one or more links will be jammed so as to deny those links for tactical use. Failure of a link does not necessarily imply network failure, since a robust network might have alternate routing and message relaying capabilities to minimize any disruptions. The same cannot be said for an LPI network, however, because it is assumed that detection of a single link compromises the entire network. Furthermore, it is conceivable that while none of the links in an LPI net is detectable, the aggregate transmissions across many links could be.

2.4.1 MALPI Network Design Issues

There are a number of issues which must be considered when designing the MALPI network. Generic network design issues include the administration of the network to ensure efficient operation and flexibility to handle a variety of contingencies, prioritization of channel resources, entry to and withdrawal from network, and message routing algorithms.

Tactical requirements, such as mobility and concealment, impose further constraints on the design of multiple access networks. The requirement for *mobility* is directly related to survivability in the tactical environment. At the link level, the need for mobility places real constraints on the size, weight, and space requirements for equipment to be used in the battlefield. There are operational considerations, as well, such as the time required for equipment assembly and disassembly, and electrical power requirements. At the network level, mobility requirements introduce problems regarding code acquisition and tracking, spatial searching, Doppler effects, and multipath propagation. The most severe impact is on network timing. *Concealment*, is also critical to survivability. LPI signal design is an example of electromagnetic concealment, while physical concealment refers to concealing the equipment from visual observation through the use of camouflage.

These tactical issues cannot be addressed independently. In fact, there is often a negative relationship between physical and electronic survivability—especially in the antenna subsystem. For example, to enhance mobility, the antenna must be kept small and simple to assemble/disassemble. This adversely affects the directivity of the antenna,

which in turn negatively impacts the electronic survivability of the system. Conversely, high gain antennas which are good for LPI purposes are typically larger and more difficult to hide or move than a simple omnidirectional vertical whip antenna, thus degrading the physical survivability.

Since the LPI network is composed of individual links, good design of the network will rely heavily on the concepts discussed earlier in this chapter. The designer of an LPI communications link has a variety of options available to reduce detectability. Using LPI system quality factors as a design tool, tradeoffs between transmitter power, antenna gains, interference suppression technology, and signaling waveforms can be evaluated. However, the LPI network designer may not have the same latitude in changing the scenario dependent factors. For example, the use of adaptive power control must consider the propagation to all intended receivers. Furthermore, omnidirectional antennas are often used to satisfy connectivity and mobility requirements, leaving waveform design as a primary tool in improving LPI.

2.4.2 Candidate Multiple Access Structures

To minimize detectability, LPI network waveforms should exhibit the same qualities as those for the point-to-point link. However, the network waveforms must also be compatible with the the chosen multiple access scheme. In other words, the structure of the multiple access network to some extent limits the type of waveforms which can be used. For example, direct sequence code division multiple access (DS-CDMA) networks employ direct sequence BPSK waveforms, while frequency hop CDMA (FH-CDMA) networks often use frequency shift keying (FSK). This suggests that some types of networks will likely be less effective than others for LPI purposes. The following network structures will be used in this research.

Frequency Division Multiple Access (FDMA)

In an FDMA network scheme, the total system bandwidth is partitioned into channels as shown in Figure 2.12. Guard bands may be used to reduce interference between adjacent channels. Advantages of FDMA are that each transmitter has dedicated access to its channel, and there is (ideally) no mutual interference. Hence, any modulation scheme could be used—in fact, each user could use a unique modulation if so desired.

The FDMA network has a number of disadvantages. For a fixed overall bandwidth, W_1, the number of potential users must be weighed against the bandwidth which can be assigned to each user. Furthermore, addition of new users to an already full network requires removal of existing users or a major restructuring of the network.
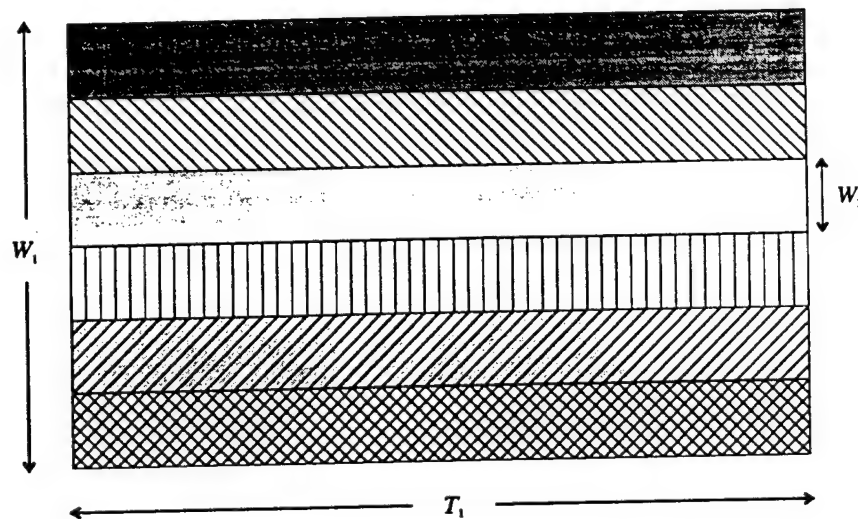
Figure 2.12: Time-Frequency Diagram for FDMA Network

Time Division Multiple Access (TDMA)

In a TDMA network, users are allocated distinct time slots, in which they have access to the entire system bandwidth, as shown in Figure 2.13. Guard times may be used to allow for timing uncertainties and signal propagation. The primary advantage of TDMA is that each user has access to a potentially much wider bandwidth than with FDMA, thus providing additional processing gain.

A primary disadvantage is the requirement for higher burst data rates to transmit a given amount of information, since transmissions are limited to the assigned time slots. Furthermore, network synchronization is required to ensure that only the authorized transmitter is active at any given time. Like FDMA, adding new users to a full network network may require removal of existing users or complete restructuring of the network.
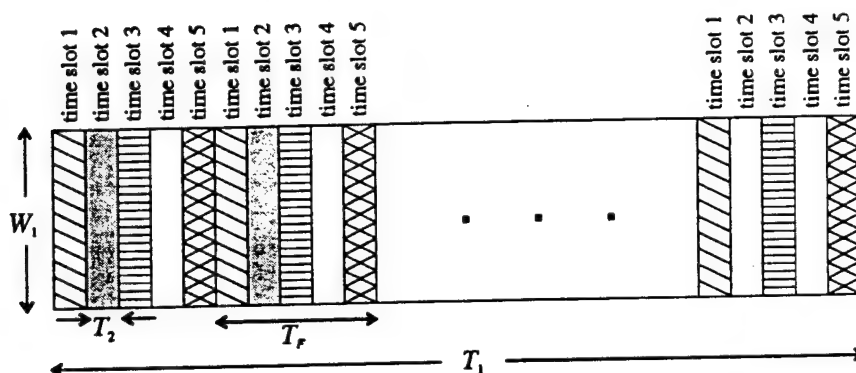
Figure 2.13: Time-Frequency Diagram for TDMA Network

Direct Sequence CDMA (DS-CDMA)

In direct sequence CDMA (DS-CDMA), each network user is assigned a unique, orthogonal DS spreading code, which is used in conjunction with BPSK modulation, as discussed in Section 2.2. The intended receivers must have the same code to demodulate the data. If every transmitter uses the same carrier frequency and bandwidth, the energy distribution in the time-frequency plane is effectively the same as that of a single DS signal, shown in Figure 2.2.

Advantages of DS-CDMA are that new users are easily added (if additional DS spreading codes are available) without changing the structure of the network, and every user has access to the entire bandwidth. Furthermore, network synchronization is not required, as in the TMDA case—synchronization is only required between the transmitter and the intended receiver(s). A disadvantage of DS-CDMA is its susceptibility to the *near-far* problem, in which strong signals prevent the reception of weaker signals.

Frequency Hop CDMA (FH-CDMA)

In an FH-CDMA network, users share the network channel resources using orthogonal frequency hop patterns, as shown in Figure 2.14. The hop patterns are assigned such that only a single user occupies a channel during a given hop period. Each user can use a variety of modulation schemes, such as frequency shift keying (FSK) or cyclic code shift keying (CCSK).

Although the FH-CDMA network resembles an FDMA/TDMA hybrid, there are several distinct advantages in using FH-CDMA [0]:

1. Privacy — If the FH code is distributed only to the intended receivers, the transmissions cannot easily be intercepted by unauthorized listeners.

2. Fading channels — In an FDMA or FDMA/TDMA network, a user who is assigned a fading position of the spectrum may experience severe degradation as long as the fading persists. With FH-CDMA, all users access the fading portion of the spectrum for a short time, and performance degradations can be readily countered by using error control coding.

3. Jam-resistance — processing gain is obtained by using the total system bandwidth, instead of the narrower channel bandwidth.

4. Flexibility — Unlike FDMA/TDMA, synchronization across the network is not required in FH-CDMA, since the orthogonality between user transmissions is not affected by transmission and propagation times. Furthermore, new users are easily added to the FH-CDMA network, provided orthogonal codes are available.
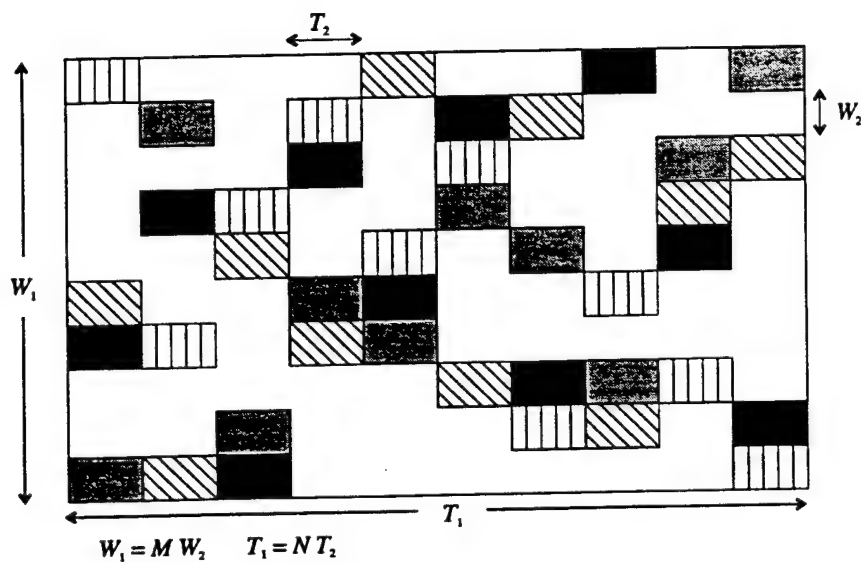
Figure 2.14: Time-Frequency Diagram for FH-CDMA Network

Chapter 3

LPI Network Detectability Models

In this chapter, the issues regarding detection and interception of MALPI networks will be explored. Detectability models and LPI metrics relating intercept performance to network signal parameters are then developed for a variety of network scenarios and intercept receivers.

3.1 Network Interception

3.1.1 General Concepts

A typical network intercept scenario is shown in Figure 3.1, in which an intercept receiver attempts to detect signal transmissions within a bandwidth W_1 over an observation interval T_1. The interceptor does not attempt to determine how many emitters are present, but rather whether or not the network is operating. For the purposes of this research, detection of any network transmissions compromises the entire network.

The idea of intercepting a network is a bit nebulous, and an obvious question is how network interception differs from the interception of a single link. What distinguishes the network intercept scenario from the link scenario presented in Chapter 2 is that the interceptor has the ability to collect and process energy from multiple sources. If the interceptor chooses to concentrate on a specific user, the intercept problem degenerates to a point-to-point LPI intercept problem, as discussed earlier.
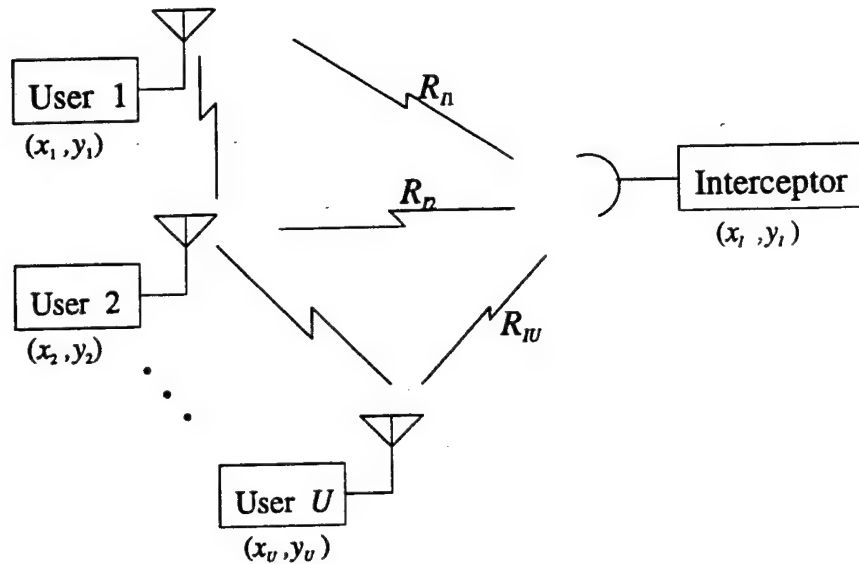
Figure 3.1: General MALPI Network Intercept Scenario

If the interceptor attempts to process energy from multiple sources, the analysis problem becomes more difficult, because the energy levels received from the various network transmitters are not constant, for two reasons: (1) directional communication and intercept antennas, and (2) the range to each transmitter may be different—for this reason the concept of "intercept range" may be meaningless in the LPI network scenario, and other performance metrics, such as intercept area, may be more descriptive.

In traditional link intercept analysis, it is assumed that the interceptor has knowledge of the signal structures and will try to exploit the energy distribution in the time-frequency plane. For example, given a choice of a channelized detector and wideband radiometer, the interceptor will use the one which gives the better performance. On the other hand, the LPI system designer selects waveform parameters such that the interceptor does not gain any such advantage. This same strategy holds for network intercept and design analysis, as well, so network detectability models and LPI performance metrics are required to facilitate the appropriate comparisons.

3.1.2 Energy Detection

All intercept receivers considered in this research are based on energy detection, so the received energy levels from each network transmitter must be determined. The total input at the intercept receiver is

$$x(t) = s_1(t) + s_2(t) + \cdots + s_U(t) + J_1(t) + J_2(t) + \cdots + J_N(t) + n(t) \qquad (3.1)$$

where $s_j(t)$ is the received signal from the jth transmitter, U is the number of active transmitters, $J_n(t)$ is the received signal from the nth jammer, and $n(t)$ is additive white Gaussian noise (AWGN) with two-sided power spectral density $N_{0I}/2$. In this research, jamming will not be considered, so $J_n(t) = 0$. Using the intercept link equations derived in Section 2.1, the received energy to noise PSD ratio from the jth emitter can be written as follows:

$$\frac{E_j}{N_{0I}} = \frac{P_{Tj}G_{TjI}G_{ITj}T_{Sj}}{N_{0I}L_{Ij}\alpha_{Ij}(f, R_{Ij})} \qquad (3.2)$$

$$= \frac{P_{Tj}G_{TjI}G_{ITj}(T_I\tau_j)}{N_{0I}L_{Ij}\alpha_{Ij}(f, R_{Ij})} \qquad (3.3)$$

where

- E_j is the received energy from the jth transmitter measured over its signal duration, T_{Sj} (i.e., $E_j = \int_0^{T_{Sj}} |s_j(t)|^2 \, dt$)

- T_{Sj} is the smaller of the signal duration and the interceptor's integration interval, T_I, and $\tau_j = T_{Sj}/T_I$

- P_{Tj} is the average power of the jth transmitter

- G_{TjI} is the antenna gain of the jth transmitter in the direction of the interceptor

- G_{ITj} is the antenna gain of the interceptor in the direction of the jth transmitter

- L_{Ij} is the atmospheric path loss in the jth intercept link

- R_{Ij} is the intercept range to the jth transmitter

- $\alpha_{Ij}(f, R_{Ij})$ is the propagation loss, in the jth intercept link, which depends on the operating frequency, f

It will be assumed that each transmitter may broadcast to several network receivers simultaneously. The required transmitter power then depends on the distance to each receive node, antenna patterns, and the desired performance level of the network. The concepts from Section 2.1 can again be used to obtain the required transmit power for the jth transmitter to transmit to the ith receiver:

$$P_{Tj} = \left(\frac{S_C}{N_{0C}} \right) \frac{N_{0C} L_{Cji} \alpha_{Cji}(f, R_{Cji})}{G_{TjCi} G_{CiTj}} \tag{3.4}$$

where

- S_C/N_{0C} is the received signal power to noise PSD required by a network receiver to obtain the specified bit error probability ($S_C/N_{0C} = R_b E_b/N_{0C}$, where R_b is the data rate)

- G_{TjCi} is the antenna gain of the jth transmitter in the direction of the ith receiver

- G_{CiTj} is the antenna gain of the ith receiver in the direction of the jth transmitter

- L_{Cji} is the atmospheric loss in the ith communication link

- R_{Cji} is the range of the ith communication link

- $\alpha_{Cji}(f, R_{Cji})$ is the propagation loss in the ith communication link

Using (3.4) in (3.2) yields

$$\frac{E_j}{N_{0I}} = T_{Sj} \left(\frac{S_C}{N_0} \right) \frac{L_{Cji}}{L_{Ij}} \frac{N_{0C}}{N_{0I}} \frac{\alpha_{Cji}(f, R_{Cji})}{\alpha_{Ij}(f, R_{Ij})} \frac{G_{TjI} G_{ITj}}{G_{TjCi} G_{CiTj}} \tag{3.5}$$

Before proceeding with the development of network detectability models, some simplifications for (3.5) are required. The simplifications deal with the type of antennas used, path losses, and the required SNR for the network receivers.

Omnidirectional Antennas

To provide maximum performance with minimal transmitter power, multiple high-gain antennas or phased array platforms could be used by each network transmitter to track

the intended receivers. This would be quite expensive and would likely impair mobility. Instead, omnidirectional antennas with 0 dB gain will be used here to provide the most flexibility and mobility in operating the network.

Propagation and Atmospheric Losses

The value of $\alpha(f, R)$, depends on the mode of propagation. For air-to-air propagation, $\alpha(f, R) = (4\pi R/\lambda)^2$, where $\lambda = c/f$ $(c = 3(10)^8$ m/s). This "free space" model is widely accepted, however it has several limitations, which are noted in [0]. First, it is only an approximate, and gives average attenuation values. Second, it assumes narrowband signals, and may not accurately predict the attenuation of all frequency components in a spread spectrum signal. Finally, it does not account for dispersion on the propagation path, which may lead to phase distortion. While this distortion is not critical to the interceptor (which uses noncoherent processing to detect the signal), it does pose problems for the communicator if large coherent bandwidths are required, such as in DS-CDMA.

For ground-to-ground propagation, the antennas are close to the earth, and the free space assumption may not be valid. If the radio horizon effects are not insignificant, the propagation attenuation factor may be expressed as [0, 0]

$$\alpha(f, R) = C(f, R_0)\alpha_{fs}(f, R_0)(R/R_0)^4 \tag{3.6}$$

where $C(f, R_0)$ is a scaling factor, which depends on a reference range, R_0 (usually 1 mile), and operating frequency, f. $\alpha_{fs}(f, R_0)$ is the free space attenuation evaluated at the same range and frequency. Typical values for $C(f, R_0)$ are given in Table 3.1 (from [0]). The minimum and maximum ranges describe the region for which (3.6) gives accurate results assuming smooth earth, vertical polarization, and soil with good conductivity properties.

The air-to-air and ground-to-ground propagation modes represent lower and upper bounds for $\alpha(f, R)$; for air-to-ground and ground-to-air propagation modes, an intermediate loss factor is applicable. For simplicity, the air-to-air free space model will be used exclusively in this research, in spite of its limitations.

The atmospheric loss factors, L_{Ij} and L_{Cji}, are also functions of range, and account for additional losses due to precipitation and water vapor. The two loss factors can

Freq (MHz)	One antenna on ground, the other height in feet	$C(f, R_0 = 1 \text{ mi})$ (dB)	R_{min} (mi)	R_{max} (mi)
30	0	28	0.1	20
30	100	15	0.4	15
60	0	34	0.1	20
60	100	15	0.5	10
150	0	42	0.1	10
150	100	15	0.1	60
300	10	35	0.1	10

Table 3.1: Values of Propagation Constant $C(f, R_0 = 1 \text{ mi})$

usually be treated as equal, since the communication and intercept ranges are approximately the same, and the receivers operate under common atmospheric conditions.

Jamming and Interference Suppression

In this research, the effects of jamming and unintentional interference will not be considered. Therefore, it will be assumed that the noise power spectral density is the same for the intercept and communication receivers ($N_{0C} = N_{0I} = N_0$).

Maximum Communication Range

When omnidirectional antennas are used, the transmit power level must be large enough to deliver the required SNR to obtain the required bit error probability at each intended receiver. The range to the furthest receiver will be denoted as R_{Cj} (hereafter referred to as the broadcast range). Any receivers which are closer than R_{Cj} will receive excess signal strength.

Using all of these assumptions, Equation (3.5) can be simplified to

$$\frac{E_j}{N_0} = T_{Sj} G_I \left(\frac{S_C}{N_0}\right) \left(\frac{R_{Cj}}{R_{Ij}}\right)^2 \tag{3.7}$$

If the interceptor is inside the network and uses an omnidirectional antenna, then

$$\frac{E_j}{N_0} = T_{Sj} \left(\frac{S_C}{N_0}\right) \left(\frac{R_{Cj}}{R_{Ij}}\right)^2 \tag{3.8}$$

Equation (3.8) is the basis for the *Dispersed Network Intercept Model* (DNIM), in which the energy received from each network transmitter depends on the ratio of the broadcast and intercept ranges.

Stand-off Intercept Scenario

A second network detectability model can be developed based on the scenario depicted in Figure 3.2. In this model, referred to as the *Stand-off Network Intercept Model* (SNIM), the interceptor is removed from the network, whose emitters are tightly clustered, or perhaps collocated. It will also be assumed that the transmitters use equal power $(R_{Cj} = R_C)$, and the interceptor uses a high gain antenna, G_I, which covers all emitters in the mainlobe.
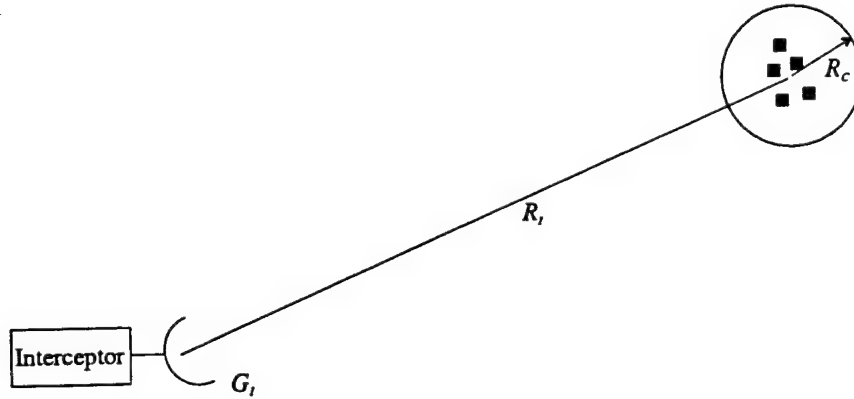
Figure 3.2: Stand-off Intercept Scenario

Since the emitters are collocated or very close together, the intercept range is approximately constant $(R_{Ij} = R_I)$. Assuming all users have equal access time to the channel $(T_{Sj} = T_S)$, the SNR received from each transmitter is constant:

$$\frac{E_j}{N_0} = T_S G_I \left(\frac{S_C}{N_0}\right) \left(\frac{R_C}{R_I}\right)^2 \tag{3.9}$$

3.2 Wideband Radiometer

3.2.1 Dispersed Network Intercept

The wideband radiometer is the logical detector of the DS-CDMA network, and it can be used for any other multiple access scheme as well: FDMA, TDMA, FH-CDMA. One approach to analyzing the detection performance of the radiometer is to determine the probability of detection, P_D, based on the available SNR, $(E/N_0)_{recv}$, and the tolerable false alarm probability, P_F. All network signals are assumed to be orthogonal, allowing direct addition of the energy received from each transmitter. For example, in the FDMA, TDMA, and CDMA networks, orthogonality is obtained by virtue of frequency, time, and code separation, respectively. Therefore, using (3.8), the total received SNR from U active transmitters is

$$\left(\frac{E}{N_0}\right)_{recv} = \sum_{j=1}^{U} T_{Sj} \frac{S_C}{N_0} \left(\frac{R_{Cj}}{R_{Ij}}\right)^2 = \sum_{j=1}^{U} \tau_j T_1 \frac{S_C}{N_0} \left(\frac{R_{Cj}}{R_{Ij}}\right)^2 \tag{3.10}$$

where $\tau_j = T_{Sj}/T_1$, and T_1 is the radiometer's integration time.

The achieved P_D can then be determined using the following relationship, known as the *full normal* approximation [0, 0]:

$$P_D = Q \left[\frac{Q^{-1}(P_F) - (E/N_0)_{recv}/\sqrt{T_1 W_1}}{\sqrt{1 + 2(E/N_0)_{recv}/T_1 W_1}} \right] \tag{3.11}$$

where W_1 is the radiometer's bandwidth. For large time-bandwidth products ($T_1 W_1 > 1000$) and small SNR ($2(E/N_0)_{recv} \ll T_1 W_1$), (3.11) can be simplified to yield the *simple normal* approximation, which is simply a rearrangement of (2.28):

$$P_D = Q \left[Q^{-1}(P_F) - \frac{(E/N_0)_{recv}}{\sqrt{T_1 W_1}} \right] \tag{3.12}$$

Alternatively, if P_D and P_F are specified, the required SNR can be determined using (2.25) or (2.28):

$$\left(\frac{E}{N_0}\right)_{req} = \frac{X_0 + \sqrt{X_0^2 + 16 T_1 W_1 X_0}}{4} \tag{3.13}$$

$$= d\sqrt{T_1 W_1}, \qquad T_1 W_1 \geq 1000 \tag{3.14}$$

where $X_0 = d^2 = [Q^{-1}(P_F) - Q^{-1}(P_D)]^2$. To meet or exceed the desired intercept performance, the total received SNR must exceed that given in (3.14):

$$\left(\frac{E}{N_0}\right)_{recv} = \sum_{j=1}^{U} \frac{E_j}{N_0} \geq \left(\frac{E}{N_0}\right)_{req} \tag{3.15}$$

Using (3.8) in (3.15) gives

$$\sum_{j=1}^{U} T_1\, \tau_j\, \frac{S_C}{N_0}\, \left(\frac{R_{Cj}}{R_{Ij}}\right)^2 \geq \left(\frac{E}{N_0}\right)_{req}$$

$$\sum_{j=1}^{U} \tau_j \left(\frac{R_{Cj}}{R_{Ij}}\right)^2 \geq \frac{(S_I/N_0)}{S_C/N_0} = Q_{MOD} \tag{3.16}$$

where $(S_I/N_0) = (1/T_1)(E/N_0)_{req}$. Equation (3.16) looks like the sum of individual LPI quality factors for each transmitter in the network. Recall that Q_{MOD} relates the relative performance of the communication and intercept receivers (i.e., P_E, P_F, and P_D).

A useful interpretation of Equation (3.10) is given in Figure 3.3. In the figure, the received SNR from four transmitters as a function of intercept location is a represented by the three-dimensional surface above the physical x-y plane. Expressing the received SNR as a function of (x, y) yields

$$\left(\frac{E}{N_0}\right)_{recv}(x, y) = \sum_{j=1}^{U} \frac{S_C}{N_0} \frac{T_{Sj} R_{Cj}^2}{(x - x_j)^2 + (y - y_j)^2} \tag{3.17}$$

where (x_j, y_j) is the coordinate of the jth transmitter. The "poles" represent the transmitters themselves. Because of the one-to-one relationship between SNR and P_D, the probability of detection could be represented in a similar fashion. Taking horizontal cuts of the surface yields detectability contours describing regions where a constant SNR (or constant P_D) is received, as shown in Figure 3.4.

Analysis of (3.16) shows that detection of the network can be achieved in two ways. First, any single transmitter is detectable if the interceptor moves close enough to that transmitter—i.e., $E_j/N_0 \geq (E/N_0)_{req}$, because R_{Cj}/R_{Ij} is large. This condition is illustrated by the 50 dB circular contours around each transmitter in Figure 3.4. Second, there may also be intermediate regions in which interception is possible due to the integration of energy from multiple sources, as shown by the 35 and 40 dB contours.
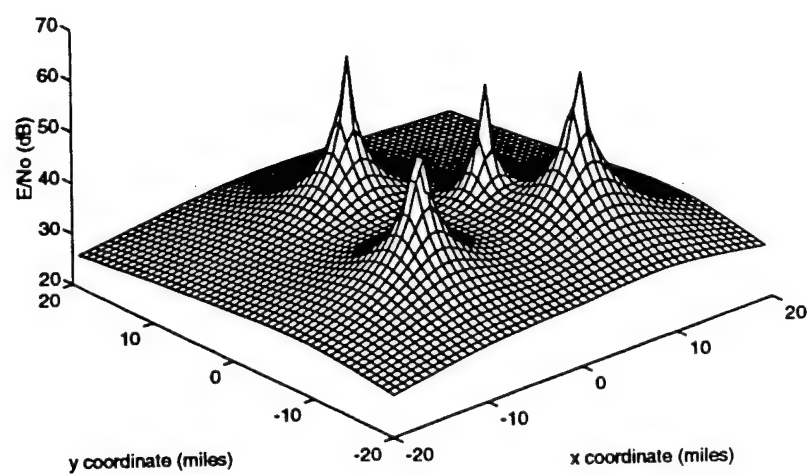
Figure 3.3: Received E/N_0 Mesh Surface
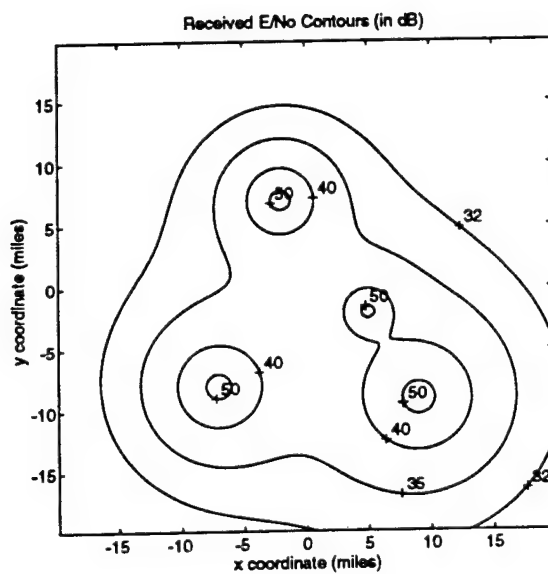
Figure 3.4: Received E/N_0 Contours

To compare the performance of one intercept receiver to another, or to assess the effect of changes in waveform parameters on network detectability, a performance metric is required. An effective measure of any LPI system, be it a single link or a network of many users, is the expected region of communications compared to the potential region of interception. For simple point-to-point LPI links, intercept range is an appropriate measure, but intercept range is somewhat meaningless in the context of the dispersed network, since each transmitter has its own intercept range.

As can be seen from Figure 3.4, intercept area, on the other hand, is an appropriate measure of network detectability for the dispersed network. For a specified P_D (or $(E/N_0)_{req}$), the intercept area is obtained by integrating the regions described by the appropriate contour lines. Unfortunately, it is difficult, and sometimes impossible, to integrate these regions analytically, except in the simplest cases, such as a single transmitter with circular P_D contours.

The intercept area can be estimated, however, by sampling the network's geographic region using an $N_X \times N_X$ grid, as shown in Figure 3.5, and determining the achieved P_D for each sample. An estimate of the intercept area is then determined as follows

$$A_{int} = \sum_{k=1}^{N_X} \sum_{l=1}^{N_X} \delta_{kl} A_{step} \tag{3.18}$$

$$\delta_{kl} = \begin{cases} 1 & , \quad P_D(k,l) \geq P_D \\ 0 & , \quad P_D(k,l) < P_D \end{cases} \tag{3.19}$$

where A_{step} is area of each sample (i.e., step size), and $P_D(k,l)$ is the achieved probability of detection, evaluated using (3.17) and (3.12) at the center of the (k,l)th sample point, (x_k, y_l). Clearly, smaller step sizes will lead to more accurate results, at the expense of increased computation time.

The total intercept area depends on a number of factors. First, the desired P_D and P_F determine the required E/N_0 for the observed time-bandwidth product, $T_1 W_1$. If three of these four parameters are held constant, then changing the fourth has the effect of raising or lowering the height of the horizontal cut of the received E/N_0 surface— which in turn reduces or increases the area of interception. For example, let T_1, P_D, and P_F be fixed. Increasing W_1 by a factor of 10 increases the required SNR by 5 dB, which could substantially reduce the area of detection, as shown by the 35 and 40 dB contours in Figure 3.4.
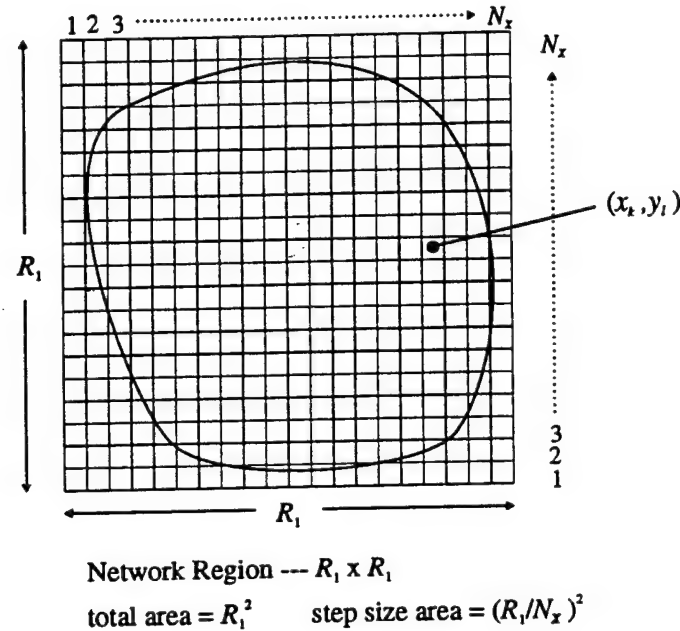
Figure 3.5: Sampling Scheme for Estimating Network Intercept Area

Likewise, each network transmitter must deliver the required S_C/N_0 to its furthest intended receiver, at a distance of R_{Cj}. Reducing S_C/N_0 through the use of modulation and coding or data rate reduction techniques (all of which are topics of Chapter 4) has the effect of lowering the entire E/N_0 surface, which for a constant $(E/N_0)_{req}$, would reduce the intercept area.

And finally, because energy from multiple sources is combined at the interceptor, the positions of the transmitters, $\{(x_j, y_j)\}$, also affect the intercept area. This is shown in Figure 3.6, in which the intercept regions are plotted as a function of transmitter separation, with the following parameters: $P_D = 0.8$, $P_F = 0.01$, $W_1 = 10$ MHz, $T_1 = 1$ sec, $(E/N_0)_{req} = 40$ dB, $R_{C1}=R_{C2}=8$ miles, $\tau_1=\tau_2=1$, and $S_C/N_0 = 30$ dB-Hz. The minimum intercept area (63 square miles) occurs when the transmitters are collocated. A maximum (80 sq miles) occurs when the separation is about 7 miles. For very large separations, the intercept area gradually converges back to the minimum.
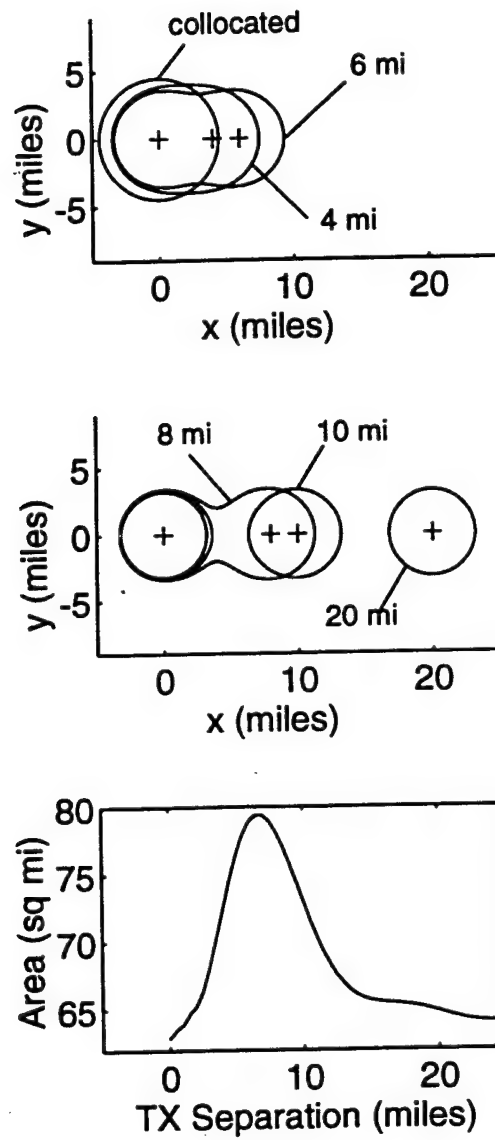
Figure 3.6: Intercept Area versus Transmitter Separation

For two emitters, rearranging (3.10) yields

$$\tau_1 \left(\frac{R_{C1}}{R_{I1}}\right)^2 + \tau_2 \left(\frac{R_{C2}}{R_{I2}}\right)^2 = \frac{(S_I/N_0)_{req}}{S_C/N_0} = Q_{MOD} \tag{3.20}$$

If the transmitters are collocated, then $x_1=x_2$, $y_1=y_2$, and $R_{I1}=R_{I2}=R_I$, in which case the network "looks like" a single transmitter with an increased power level. Solving for R_I^2 yields

$$R_I^2 = \frac{\tau_1 R_{C1}^2 + \tau_2 R_{C2}^2}{Q_{MOD}} \tag{3.21}$$

resulting in a minimum intercept area of

$$A_{min} = \pi R_I^2 = \frac{\pi}{Q_{MOD}} \left(\tau_1 R_{C1}^2 + \tau_2 R_{C2}^2\right) \tag{3.22}$$

Using the parameters for Figure 3.6,

$$A_{min} = \pi \frac{(S_C/N_0)}{(S_I/N_0)} \left(\tau_1 R_1^2 + \tau_2 R_2^2\right) = \frac{\pi}{10} \, 200 \approx 63 \text{ sq miles}$$

If the transmitters are very far apart, then the interceptor can only achieve detection when it is near one emitter. In this situation, the problem degenerates to simple link intercepts, with circular contours around each transmitter. The intercept radii, R_{I1} and R_{I2}, must satisfy the single LPI link intercept condition, hence

$$Q_{MOD} = \frac{\tau_1 R_{C1}^2}{R_{I1}^2} = \frac{\tau_2 R_{C2}^2}{R_{I2}^2} \tag{3.23}$$

yielding an intercept area of

$$A_{min} = \pi (R_{I1}^2 + R_{I2}^2) = \frac{\pi}{Q_{MOD}} \left(\tau_1 R_{C1}^2 + \tau_2 R_{C2}^2\right) \tag{3.24}$$

which is the same result as for collocated transmitters.

For the general case of U transmitters, it is easily shown that the minimum intercept area occurs when the transmitters are collocated and/or very part. Hence,

$$A_{min} = \frac{\pi}{Q_{MOD}} \sum_{j=1}^{U} \tau_j R_{Cj}^2 \tag{3.25}$$

These results suggest that transmitter placement should be a consideration when designing or operating an LPI network—i.e., for the two-transmitter network discussed earlier, a separation of 7 miles should be avoided to minimize detectability. Solving for the conditions which yield the maximum intercept area is quite complicated, however, and is beyond the scope of this research.

3.2.2 Stand-off Radiometer

The stand-off intercept scenario allows further simplification of the network detection problem, providing additional insight into the relationships among the network load, waveforms, and detectability. Using (3.9) the total received SNR is

$$\left(\frac{E}{N_0}\right)_{recv} = UT_S G_I \frac{S_C}{N_0}\left(\frac{R_C}{R_I}\right)^2 \tag{3.26}$$

Solving for the intercept range yields

$$R_I^2 = UT_S G_I R_C^2 \frac{(S_C/N_0)}{(E/N_0)_{recv}} \tag{3.27}$$

The radiometer achieves its desired performance when $(E/N_0)_{recv} \geq (E/N_0)_{req}$. Hence, the intercept range is upper bounded as follows:

$$R_I^2 \leq R_{Imax}^2 \;=\; UT_S G_I R_C^2 \frac{(S_C/N_0)}{(E/N_0)_{req}} \tag{3.28}$$

$$\;=\; \tau U G_I R_C^2 \frac{(S_C/N_0)}{(S_I/N_0)} \tag{3.29}$$

where $\tau = T_S/T_1$. The *network LPI quality factor* for the wideband radiometer is then defined as follows:

$$Q_{LPIN} \;=\; \left(\frac{R_C}{R_{Imax}}\right)^2 \tag{3.30}$$

$$\;=\; \frac{(S_I/N_0)}{(S_C/N_0)}\frac{1}{\tau U G_I} \tag{3.31}$$

$$\;=\; \frac{Q_{MOD}}{\tau U G_I} \tag{3.32}$$

where

$$\frac{S_I}{N_0} = \frac{1}{T_1}\left(\frac{E}{N_0}\right)_{req} = \left[Q^{-1}(P_F) - Q^{-1}(P_D)\right]\sqrt{\frac{W_1}{T_1}} \qquad T_1 W_1 \geq 1000 \tag{3.33}$$

From (3.32), it is clear that the multiple emitters appear as a single composite transmitter operating with a higher power level or data rate, as shown:

$$\left(\frac{R_C}{R_{Imax}}\right)^2 = \frac{(S_I/N_0)}{(U R_b)(E_b/N_0)}\frac{1}{\tau G_I}$$
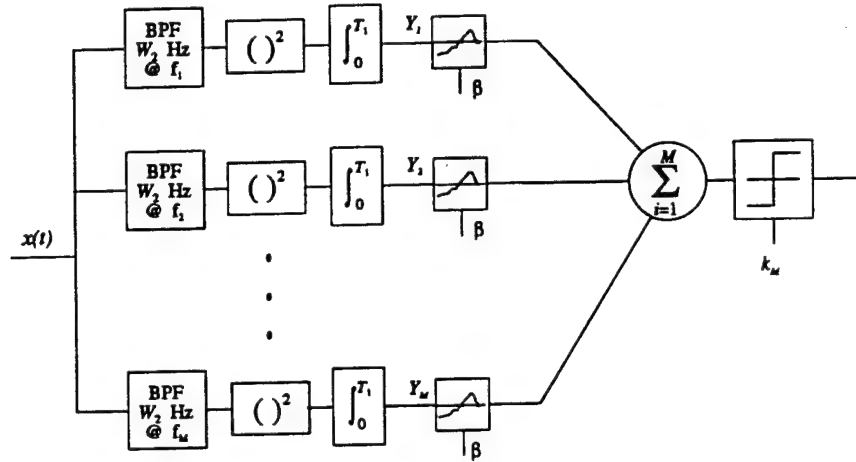
Figure 3.7: Filter Bank Detector for FDMA Networks

The detector shown in Figure 3.7 is known as a *double threshold* detector, because of the binary integration and thresholding with k_M. It has been shown that $k_M = 0.5U$ generally provides good performance [0, 0]. It is assumed here, however, that the interceptor does not know how many transmitters are active, so a threshold of $k_M = 1$ will be used, which is equivalent to ORing the channel outputs.

The overall P_F is the probability that one or more channels has a false alarm, when in fact none have signal:

$$P_F = \sum_{j=1}^{M} \binom{M}{j} Q_F^j (1 - Q_F)^{M-j} \qquad (3.35)$$

Alternatively, P_F is the complement of the probability that none of the channels has a false alarm,

$$P_F = 1 - (1 - Q_F)^M \qquad (3.36)$$

For a specified P_F, the allowable channel false alarm probability is then

$$Q_F = 1 - (1 - P_F)^{1/M} \qquad (3.37)$$

The overall P_D is the probability that one or more channels has a detection, when U channels actually have signal. The interceptor does not know which channels have

signal, and the received energy levels are different. However, since $k_M = 1$, the overall P_D is

$$
\begin{aligned}
P_D &= 1 - \text{Pr[no detections given } U \text{ signals present]} \\
&= 1 - \text{Pr[no false alarms in } M - U \text{ channels] Pr}[U \text{ missed detections]} \\
&= 1 - (1 - Q_F)^{M-U} \prod_{j=1}^{U}(1 - Q_{Dj})
\end{aligned}
\tag{3.38}
$$

where Q_{Dj} is given in (3.34).

Equation (3.38) is the dispersed network intercept model for the filter bank detector. The channel false alarm probability Q_F is determined using (3.37). Then, for the given intercept location (x, y), the received SNR from each transmitter, E_j/N_0, is determined, which allows computation of the corresponding detection probability, Q_{Dj}, using (3.34). Finally, the total intercept area can be estimated using (3.19).

3.3.2 Stand-off Filter Bank Detector

Because the received signal-to-noise ratios from the emitters are equal, all channels containing signal energy will have the same probability of detection (i.e., $Q_{Dj} = Q_D$). Therefore, given a desired overall P_D, the required Q_D is determined from (3.38): [1]

$$
Q_D = 1 - \left[\frac{1 - P_D}{(1 - Q_F)^{M-U}} \right]^{1/U}
\tag{3.39}
$$

Using (3.8) and (3.14), an upper bound on the intercept range is then determined,

$$
R_I^2 \leq R_{Imax}^2 = \tau G_I R_C^2 \frac{(S_C/N_0)}{(S_I/N_0)}
\tag{3.40}
$$

where $\tau = T_S/T_1$. The *the network LPI quality factor* for the filter bank detector is then defined as

$$
Q_{LPIN} = \left(\frac{R_C}{R_{Imax}} \right)^2 = \frac{(S_I/N_0)}{(S_C/N_0)} \frac{1}{\tau G_I}
\tag{3.41}
$$

where

$$
\frac{S_I}{N_0} = \frac{1}{T_1} \left(\frac{E}{N_0} \right)_{req} \approx \left[Q^{-1}(Q_F) - Q^{-1}(Q_D) \right] \sqrt{\frac{W_2}{T_1}} \qquad T_1 W_2 \geq 1000
\tag{3.42}
$$

---

[1] Although equal energy levels are received from the emitters, the binary OR operation on the filter bank detections is still appropriate since the number of channels containing signals is unknown

Note that there is not a direct relationship between the number of emitters and the overall detectability, as with the wideband radiometer (see (3.33)). In all of the binary detectors covered in this research, the effect of the number of users lies in the relationship between the overall performance (P_F, P_D) and the channel probabilities (Q_F, Q_D).

3.4 TDMA Network—Time Slot Detector

3.4.1 Dispersed Network Intercept

Because of its signal structure, the TDMA network is susceptible to the time slot detector, shown in Figure 3.8. It is assumed that the overall observation time, T_1, is matched to the network frame time, in which every user has a turn at the channel. The duration of each time slot is $T_2 = T_1/N$, and the overall bandwidth is W_1.
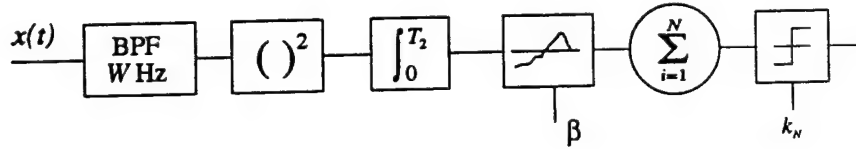
Figure 3.8: Time Slot Detector for TDMA Networks

Like the filter bank detector presented earlier, the binary moving window detector is a double threshold detector, and the optimum threshold k_N depends on the number of time slots containing signal energy, U; therefore, the number of users must be known to optimize k_N. Again, it is assumed the interceptor does not have this knowledge, so $k_N = 1$, resulting in a simple logical OR operation on the N time slot decisions. For a desired overall P_F, the allowable time slot probability of false alarm is

$$Q_F = 1 - (1 - P_F)^{1/N} \tag{3.43}$$

The overall probability of detection is the probability that one or more time slot decisions result in detections, when U slots actually have signal. The received energy from each transmitter is different, so the probability of detection for each time slot,

Q_{Dj}, varies. The overall probability of detection is obtained by modifying (3.38))

$$P_D = 1 - (1 - Q_F)^{N-U} \prod_{j=1}^{U}(1 - Q_{Dj}) \tag{3.44}$$

where

$$Q_{Dj} = Q\left[Q^{-1}(Q_F) - \frac{E_j/N_0}{\sqrt{T_2 W_1}}\right] \tag{3.45}$$

and E_j/N_0 is given in (3.8).

Equation (3.44) is the dispersed network intercept model for the time slot detector. The time slot false alarm probability, Q_F, is determined using (3.43), which is then used with E_j/N_0 to determine Q_{Dj} for each time slot containing signal. The intercept area for a required P_D is estimated using (3.19).

3.4.2   Stand-off Time Slot Detector

Analysis of the stand-off time slot detector proceeds almost identically to that of the stand-off filter bank detector. Its network LPI quality factor is easily shown to be

$$Q_{LPIN} = \left(\frac{R_C}{R_{Imax}}\right)^2 = \frac{(S_I/N_0)}{(S_C/N_0)}\frac{1}{\tau G_I} \tag{3.46}$$

where $\tau = T_S/T_2$, and

$$\frac{S_I}{N_0} = \frac{1}{T_2}\left(\frac{E}{N_0}\right)_{req} = \left[Q^{-1}(Q_F) - Q^{-1}(Q_D)\right]\sqrt{\frac{W_1}{T_2}} \qquad T_2 W_1 \geq 1000 \tag{3.47}$$

and

$$Q_D = 1 - \left[\frac{1 - P_D}{(1 - Q_F)^{N-U}}\right]^{1/U} \tag{3.48}$$

Recall that in TDMA networks, S_C/N_0 must be increased by a factor of N to account for the higher data rates.

3.5   FH-CDMA Network—FB/BMW Detector

3.5.1   Dispersed Network Intercept

There are several methods for detecting the FH-CDMA network scheme. Options include simple radiometric detection on the $W_1 \times T_1$ time-frequency space, filter bank
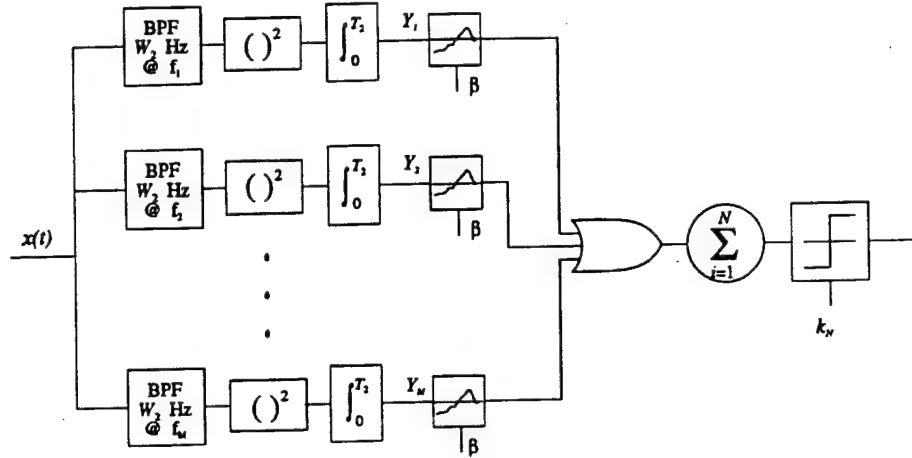
Figure 3.9: Filter Bank/Binary Moving Window Detector for FH-CDMA Networks

detection on $W_2 \times T_1$, hop rate detection on $W_1 \times T_2$, and the filter bank/binary moving window (FB/BMW) detector, shown in Figure 3.9.

As its name implies, the FB/BMW detector is a filter bank detector, applied to each hop interval, followed by an accumulator and thresholding. The bandwidth and integration of the radiometers are matched to the hop rate and channel bandwidth (see Figure 2.14). The binary OR gate is appropriate since the number of frequency channels in use is assumed to be unknown.

The signal and noise statistics are assumed constant for each hop interval, so the overall probabilities of false alarm and detection are

$$P_F = \sum_{i=k_N}^{N} \binom{N}{i} p_0^i (1 - p_0)^{N-i} \tag{3.49}$$

$$P_D = \sum_{i=k_N}^{N} \binom{N}{i} p_1^i (1 - p_1)^{N-i} \tag{3.50}$$

where p_0 is the probability that a "1" enters the binary moving window when only noise is present in a hop interval, and p_1 is the probability that a "1" enters the window when one or more signals are present. Typical values for k_N are $0.5N$-$0.6N$.

At this point, the analysis proceeds identically to that of the filter bank detector, described in Section 3.3. Using the binary OR operation to combine the filter bank

outputs, p_0 and p_1 are given as

$$p_0 = 1 - (1 - Q_F)^M \tag{3.51}$$

$$p_1 = 1 - (1 - Q_F)^{M-U} \prod_{j=1}^{U} (1 - Q_{Dj}) \tag{3.52}$$

where

$$Q_{Dj} = Q\left[Q^{-1}(Q_F) - \frac{E_j/N_0}{\sqrt{T_2 W_2}}\right] \tag{3.53}$$

and E_j/N_0 is given in (3.8) and $T_{Sj} \leq T_2$.

$$Q_F = 1 - (1 - p_0)^{1/M} \tag{3.54}$$

$$\tag{3.55}$$

Equation (3.50) is the dispersed network intercept model for FB/BMW detection. Use of the model is summarized as follows: First, the hop false alarm probability, p_0, is solved using (3.51), which is used to determine Q_F. Then, for a given intercept location (x, y), the received SNR from each transmitter, E_j/N_0, and corresponding detection probability, Q_{Dj}, are determined using (3.8) and (3.53). The overall intercept area can then be estimated using (3.19).

3.5.2 Stand-off FB/BMW Detector

Development of the network LPI quality factor for the stand-off FB/BMW detector proceeds similar to that of the filter bank detector, resulting in

$$Q_{LPIN} = \left(\frac{R_C}{R_{Imax}}\right)^2 = \frac{(S_I/N_0)}{(S_C/N_0)} \frac{1}{\tau G_I} \tag{3.56}$$

where $\tau = T_S/T_2$, and

$$\frac{S_I}{N_0} = \frac{1}{T_2}\left(\frac{E}{N_0}\right)_{req} = \left[Q^{-1}(Q_F) - Q^{-1}(Q_D)\right]\sqrt{\frac{W_2}{T_2}} \qquad T_2 W_2 \geq 1000 \tag{3.57}$$

Given P_F and P_D, the appropriate p_0 and p_1 are solved numerically using (3.49) and (3.50). The channel false alarm and detection probabilities are then determined using (3.54) and

$$Q_D = 1 - \left(\frac{1 - p_1}{(1 - Q_F)^{M-U}}\right)^{1/U} \tag{3.58}$$

WB Radiometer	$P_D = Q\left[Q^{-1}(P_F) - \frac{(E/N_0)_{recv}}{\sqrt{T_1 W_1}}\right]$
	$(E/N_0)_{recv} = T_1(S_C/N_0)\sum_{j=1}^{U}\tau_j(R_{Cj}/R_{Ij})^2$ $\tau_j = T_{Sj}/T_1$ $R_{Ij}^2 = (x_I - x_j)^2 + (y_I - y_j)^2$
Filter Bank M channels	$P_D = 1 - (1 - Q_F)^{M-U}\ \prod_{j=1}^{U}(1 - Q_{Dj})$ $Q_{Dj} = Q\left[Q^{-1}(Q_F) - \frac{E_j/N_0}{\sqrt{T_1 W_2}}\right]$ $E_j/N_0 = T_2(S_C/N_0)\tau_j(R_{Cj}/R_{Ij})^2$ $Q_F = 1 - (1 - P_F)^{1/M}$ $\tau_j = T_{Sj}/T_1,\ M = W_1/W_2$
Time Slot N time slots	$P_D = 1 - (1 - Q_F)^{N-U}\ \prod_{j=1}^{U}(1 - Q_{Dj})$ $Q_{Dj} = Q\left[Q^{-1}(Q_F) - \frac{E_j/N_0}{\sqrt{T_2 W_1}}\right]$ $E_j/N_0 = T_2(S_C/N_0)\tau_j(R_{Cj}/R_{Ij})^2$ $Q_F = 1 - (1 - P_F)^{1/N}$ $\tau_j = T_{Sj}/T_2,\ N = T_1/T_2$
FB/BMW Detector M channels N hops	$P_D = \sum_{i=k_N}^{N}\binom{N}{i}p_1^i(1 - p_1)^{N-i}$ $P_F = \sum_{i=k_N}^{N}\binom{N}{i}p_0^i(1 - p_0)^{N-i}$ $p_0 = 1 - (1 - Q_F)^M$ $p_1 = 1 - (1 - Q_F)^{M-U}\ \prod_{j=1}^{U}(1 - Q_{Dj})$ $Q_F = 1 - (1 - p_0)^{1/M}$ $Q_{Dj} = Q\left[Q^{-1}(Q_F) - \frac{E_j/N_0}{\sqrt{T_2 W_2}}\right]$ $\tau_j = T_{Sj}/T_2,\ N = T_1/T_2,\ M = W_1/W_2$

Table 3.2: Detectability Calculations for the Dispersed Network Intercept Model

Receiver Type	*Network Quality Factor*
WB Radiometer $(\tau = T_S/T_1)$	$Q_{LPIN} = \frac{(S_I/N_0)}{(S_C/N_0)} \frac{1}{U\tau G_I}$ $(S_I/N_0) = (Q^{-1}(P_F) - Q^{-1}(P_D)) \sqrt{W_1/T_1}$
Binary Detectors **Filter Bank** $(\tau = T_S/T_1)$	$Q_{LPIN} = \frac{(S_I/N_0)}{(S_C/N_0)} \frac{1}{\tau G_I}$ $(S_I/N_0) = [Q^{-1}(Q_F) - Q^{-1}(Q_D)] \sqrt{W_2/T_1}$ $Q_F = 1 - (1 - P_F)^{1/M}$ $Q_D = 1 - \left(\frac{1-P_D}{(1-Q_F)^{M-U}}\right)^{1/U}$
Time Slot $(\tau = T_S/T_2)$	$(S_I/N_0) = [Q^{-1}(Q_F) - Q^{-1}(Q_D)] \sqrt{W_1/T_2}$ $Q_F = 1 - (1 - P_F)^{1/N}$ $Q_D = 1 - \left(\frac{1-P_D}{(1-Q_F)^{N-U}}\right)^{1/U}$
FB/BMW Detector $(\tau = T_S/T_2)$	$(S_I/N_0) = [Q^{-1}(Q_F) - Q^{-1}(Q_D)] \sqrt{W_2/T_2}$ $Q_F = 1 - (1 - p_0)^{1/M}$ $Q_D = 1 - \left(\frac{1-p_1}{(1-Q_F)^{M-U}}\right)^{1/U}$ $P_F = \sum_{i=k_N}^{N} \binom{N}{i} p_0^i (1 - p_0)^{N-i}$ $P_D = \sum_{i=k_N}^{N} \binom{N}{i} p_1^i (1 - p_1)^{N-i}$ $k_N = 0.6N$

Table 3.3: Summary of Network LPI Quality Factors

3.6 Detectability Comparisons

Tables 3.2 and 3.3 summarize the dispersed and stand-off network intercept models. In this section, the detectability of several candidate multiple access schemes will be evaluated to illustrate the use of these models.

3.6.1 Constraints for Comparison

In LPI link analysis, the comparison of different intercept receivers is usually accomplished by analyzing their relative intercept ranges for a fixed performance level. These comparisons are easily made using the quality factors, as introduced in Chapter 2. When the waveform parameters are fixed (i.e., data rate, modulation, and bandwidth), it is sufficient to compare the required signal-to-noise ratios required for detection.

The problem of comparing one network scheme to another (such as FDMA versus DS-CDMA) however, is slightly more involved, and any comparisons should ensure consistency among network parameters. Therefore, in these examples, the following parameters will be fixed:

- Total bandwidth, W_1, and observation interval T_1

- Total capacity, N_U (maximum number of users)

- Average data rate per user, R_b, as measured over the observation interval, T_1

- Transmitter locations, (x_j, y_j), and broadcast ranges, R_{Cj}

By fixing these parameters, any differences in the detectability of the networks will be due to the multiple access structures (i.e., waveforms) and the methods used to detect them (i.e., wideband versus channelized).

3.6.2 Lightly Loaded Network—Dispersed Model

In this section, the detectability of several networks are compared for a situation in which a small number of transmitters are operating. The parameters given in Table 3.4 will be used.

$N_U = 20$ users, maximum	$U = 4$ active users ($U/N_U = 20\%$)
$W_1 = 10$ MHz	$T_1 = 1$ sec
$R_{Cj} = 10$ miles	(x_j, y_j) randomly distributed
$P_E = 10^{-5}$ bit error prob	$R_b = 100$ bps average data rate
$P_F = 10^{-4}$ false alarm prob	$P_D = 0.95$ detection probability
$G_I = 0$ dB (omnidirectional antenna)	

Table 3.4: Constraints for Lightly Loaded Network Comparison

FDMA

To support the maximum number of users, the FDMA network must have $M = N_U = 20$ channels; if the channels are contiguous then $W_2 = W_1/M$. The interceptor does not know which of the channels are in use, so all must be covered. Each transmitter could conceivably use a distinct form of modulation, as long as the transmitted waveform is restricted to that transmitter's allocated bandwidth. However, it will be assumed that all emitters use BPSK with 100% duty cycles. DS spreading is used to fill out the 10 MHz bandwidth.

Assuming there are no implementation losses, direct sequence spreading is a reversible process, and the bit error probability depends solely on the bit energy to noise ratio. To obtain $P_E = 10^{-5}$, an SNR of $E_b/N_0 = 9.6$ dB is required. With an average data rate of $R_b = 100$ bps, the required signal power to noise ratio is $S_C/N_0 = 29.6$ db-Hz. The transmitters are distributed randomly in a 400 square mile region, 20 miles to a side—their coordinates, $\{(x_j, y_j)\}$, were drawn from a uniform distribution over $[-10, 10]$.

Figure 3.10 shows the detectability contours for $P_D = 0.95$. The network intercept areas for the radiometer and filter bank detector are 83 and 254 square miles, respectively. In terms of intercept area, the filter bank detector presents the greater threat to this particular network.

TDMA

To support the maximum number of users, the TDMA network must provide $N = N_U = 20$ time slots during the observation time T_1, hence $T_2 = T_1/N$ sec. BPSK with

Detectability Contours, FDMA Network Example #1
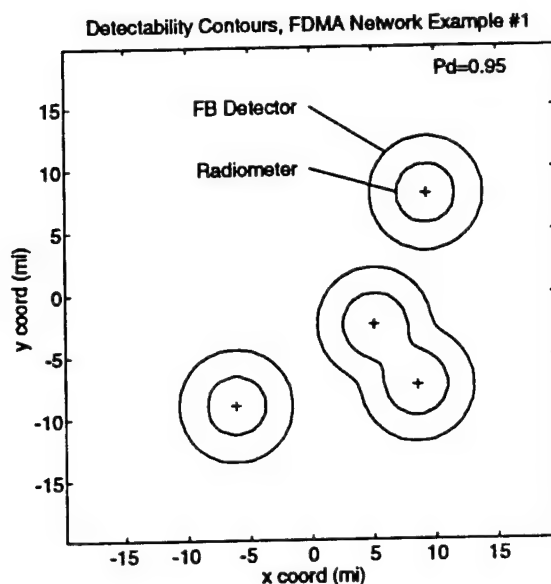
Figure 3.10: Detectability Comparison for FDMA Network

DS spreading modulation will be assumed. To account for the reduced channel access time, each user's effective data rate must be increased by a factor of $N = 20$, leading to an increase in S_C/N_0 by 13 dB. However, the received energy from each transmitter is unchanged, since the duration of each signal is reduced by a factor of 20. This important result leads to the equivalence of FDMA and TDMA detectability for a given maximum capacity and modulation format, which will be discussed later in more detail.

Figure 3.11 shows the detectability results for the lightly loaded TDMA network, with $S_C/N_0 = 42.6$ dB-Hz. The detection area for $P_D = 0.95$ was 83 square miles for the wideband radiometer and 254 square miles for the time slot detector, which agree with the FDMA results.

DS-CDMA

The number of users operating in a direct-sequence CDMA network is limited primarily by the availability of orthogonal spreading codes. There are practical limitations to the number of transmitters, as well, such as the *near-far* problem, in which strong
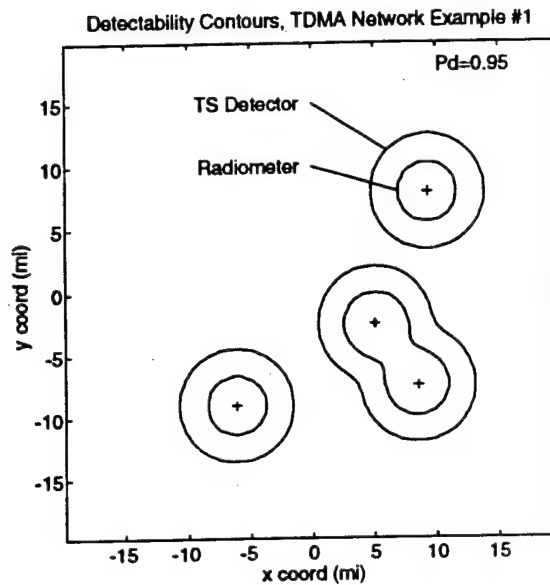
Figure 3.11: Detectability Comparison for TDMA Network

signals interfere with reception of weaker signals. Note that both of these constraints are communication, rather than interception, issues; it will be assumed here that a sufficient number of spreading codes are available, and that the near-far problem does not exist.

If each transmitter employs BPSK modulation with direct sequence spreading to fill out the bandwidth W_1, then $E_b/N_0 = 9.6$ dB for $P_E = 10^{-5}$, and $S_C/N_0 = 29.6$ db-Hz. An appropriate detector for the DS-CDMA network is the wideband radiometer, which provides the same detectability as for the FDMA network determined earlier, since the two networks are equivalent in terms of the total bandwidth observed, data rates, and modulation. The only difference between the networks is how the energy is distributed within the overall bandwidth—frequency versus code division—the wideband radiometer is oblivious to this distribution, since the signals are orthogonal.

Frequency-Hopping CDMA

In the FH-CDMA network, multiple users access the channel using orthogonal frequency hopping patterns, as described earlier. If $1/T_2$ is the frequency hop rate, then $N = T_1/T_2$ hops are observed. To support the maximum number of users, the network must have $M = N_U = 20$ channels; if the channels are contiguous, $W_2 = W_1/M$. Because of the multiple access structure of the network, the transmitted waveforms must be compatible with a frequency hopping modulation scheme, such as frequency shift keying (FSK) or cyclic code shift keying (CCSK). Noncoherent detection methods are often used for practical reasons.

For this example, 32-ary orthogonal FSK with noncoherent detection will be used with a hop rate of $1/T_2 = 20$ hops/sec, hence $N = 20$. Since each hop contains five bits of information, a total of 100 bits are transmitted in the T_1 time frame, yielding the required data rate of 100 bps per user. For $P_E = 10^{-5}$, $E_b/N_0 = 7.1$ dB, and $S_C/N_0 = 27.1$ dB-Hz.

Detectability contours for the wideband radiometer and FB/BMW detector are shown in Figure 3.12. The detection area for the two detectors are 41 and 74 square miles, respectively, again showing that the channelized detector poses the greater threat for a lightly loaded network.

3.6.3 Lightly Loaded Network–Stand-off Intercept

Using Table 3.3, the network LPI quality factors for the various networks and receivers can be determined as follows: First, for interception of an FDMA network using the wideband radiometer, $S_I/N_0 = 42.3$ dB-Hz and $S_C/N_0 = 29.6$ dB-Hz. Hence $Q_{LPIN} = 42.3 - 29.6 - 10\log(U) = 6.7$ dB. For the filter bank detector, $S_I/N_0 = 35$ dB-Hz, hence $Q_{LPIN} = 35 - 29.6 = 5.4$ dB, showing that the filter bank detector performs slightly better than the radiometer, which is consistent with the results from the dispersed network example.

With TDMA, S_C/N_0 is increased by 13 dB to account for the higher data rate. For the radiometer, $S_I/N_0 = 42.3$ dB-Hz, and $\tau = 0.05$; therefore $Q_{LPIN} = 42.3 - 42.6 - 10\log(U) - 10\log(0.05) = 6.7$ dB, which is the same result as for FDMA. Likewise, for the time slot detector, $S_I/N_0 = 48$ dB-Hz, hence $Q_{LPIN} = 48 - 42.6 = 5.4$ dB,
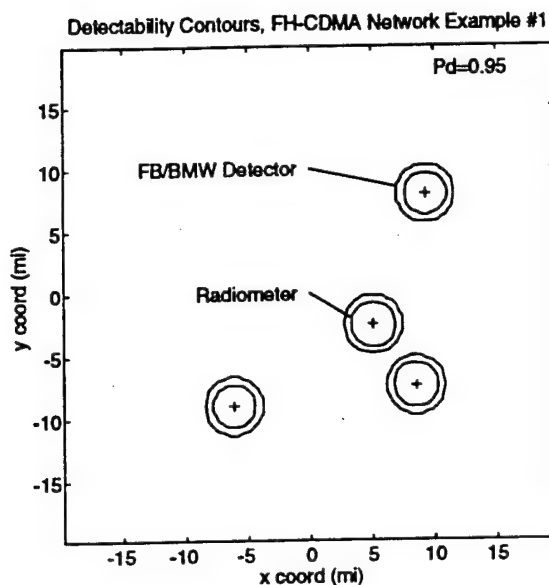
Figure 3.12: Detectability Comparison for FH-CDMA Network

equivalent to filter bank detection of the FDMA network.

For FH-CDMA, $S_C/N_0 = 27.1$ dB-Hz using 32-ary orthogonal FSK and noncoherent detection. The radiometer quality factor is therefore $Q_{LPIN} = 9.2$ dB. For the FB/BMW detector, $S_I/N_0 = 37.1$ dB-Hz, and $Q_{LPIN} = 10$ dB, which means that the radiometer is slightly better when the network transmitters are collocated.

3.6.4 Heavily Loaded Network—Dispersed Model

The parameters in Table 3.5 will be used for this example, in which fully-loaded networks will be used. Here, "fully-loaded" means that the maximum number of users are active— i.e., all channels or time slots are in use. Again, the transmitter locations are drawn from a uniform distribution, although the same locations are used in each network scheme.

Figure 3.13 shows the results for the fully-loaded FDMA network. For $P_D = 0.95$, the detection areas using the wideband radiometer and filter bank detector were 913 and 841 square miles, respectively.

As discussed in the previous example, the detectability of the TDMA network is

$N_U = 20$ users, maximum	$U = 20$ active users (100% load)
$W_1 = 100$ MHz	$T_1 = 1$ sec
$R_{Cj} = 8$ miles	(x_j, y_j) randomly distributed
$P_E = 10^{-5}$ bit error prob	$R_b = 1000$ bps data rate
$P_F = 10^{-4}$ false alarm prob	$P_D = 0.95$ detection probability
$G_I = 0$ dB (omnidirectional antenna)	

Table 3.5: Constraints for Fully-Loaded Network Comparison

equivalent to that of the FDMA network. Adding more emitters does not affect this duality, so the detection performance of the wideband radiometer is the same for the two networks. Likewise, the time slot detector provides the same performance as the filter bank detector in the FDMA scenario.

Figure 3.14 shows the detection results for the fully-loaded FH-CDMA network. 32-ary orthogonal FSK with noncoherent detection was again assumed, so for an average data rate of 1000 bps, $N = 200$ hops are observed over the 1 second observation period. The detection areas for the wideband radiometer and FB/BMW detectors for $P_D = 0.95$ were 615 and 406 square miles, respectively. Note that for the network parameters used in this example, the radiometer provides substantially better performance than the FB/BMW detector.

Detectability Contours, FDMA Network Example #2

Pd=0.95

Radiometer

y coord (mi)

x coord (mi)
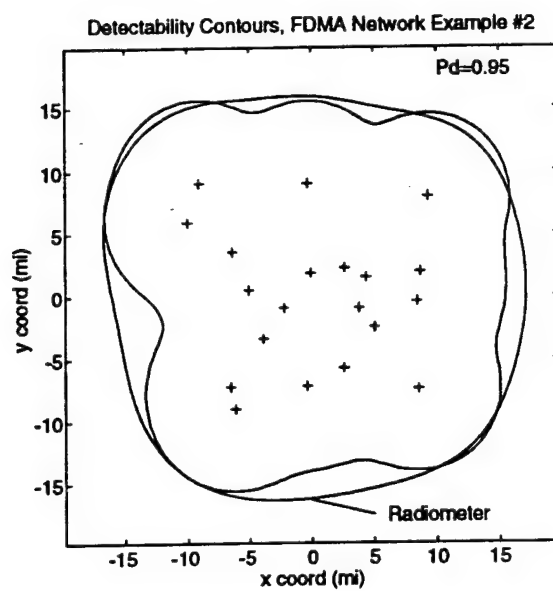
Figure 3.13: Detectability Comparison for FDMA Network (Fully Loaded)

Detectability Contours, FH-CDMA Network Example #2
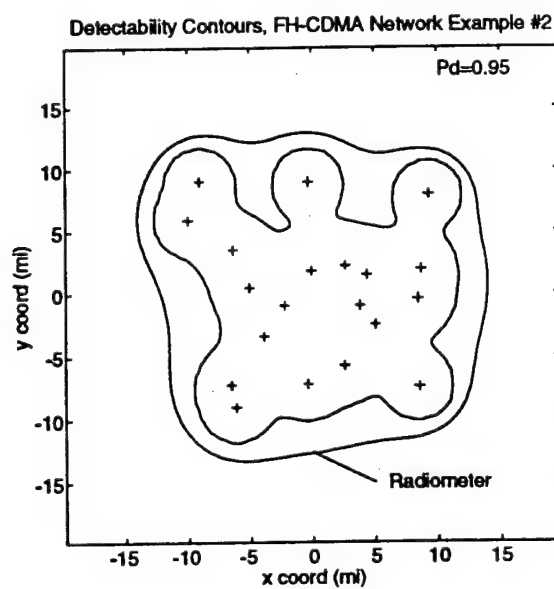
Pd=0.95

Radiometer

y coord (mi)

x coord (mi)

Figure 3.14: Detectability Comparison for FH-CDMA Network (Fully-Loaded)

3.6.5   Heavily Loaded Network—Stand-Off Interceptor

Quality factors for the stand-off intercept model using the parameters in Table 3.5 are given as follows:

- FDMA, wideband radiometer: 4.7 dB,   filter bank: 9.1 dB (radiometer presents the greater threat)

- TDMA — same as FDMA

- FH-CDMA, wideband radiometer: 7.2 dB,   FB/BMW: 11.7 dB (radiometer presents the greater threat)

At first glance, these results seem to conflict with the results from the dispersed model. For example, in the dispersed FDMA network, the radiometer and filter bank detectors provide approximately the same intercept area. In the stand-off scenario, however, the radiometer's quality factor is 4.4 dB higher, which translates to a 2.2 dB range difference—i.e., the radiometer's detection range is roughly 1.7 times as large as that of the filter bank detector.

One reason for this apparent disparity is that the filter bank detector's performance is dominated by the channel(s) receiving energy from the closest transmitters, as evidenced by the P_D contours in Figure 3.13—the same effect occurs in the FB/BMW detector, as shown in Figure 3.14. In contrast, the radiometer is more efficient, since the energy received from all network transmitters is used to form the detection decision. This issue of wideband versus filter bank detection is explored in more detail in Chapter 4.

3.6.6   Duality between FDMA and TDMA

As seen in the previous sections, a duality exists between FDMA and TDMA. From an LPI detectability standpoint, there is no advantage in using FDMA as opposed to TDMA, and vice-versa. This applies to detection with a wideband radiometer and the binary detection schemes.

Let $T_1 \times W_1$ define the overall time-frequency space of the network. To support a maximum of M users, an FDMA scheme would require M channels of bandwidth

$W_2 = W_1/\dot{M}$ Hz, while a TDMA network requires M time slots of duration $T_2 = T_1/M$:

$$
\begin{aligned}
T_1 W_1 \;&= T_1 \,(M W_2) && \text{FDMA channels} \\
&= (M T_2)\, W_1 && \text{TDMA time slots}
\end{aligned}
$$

For a dispersed network with U emitters, the total SNR received by a wideband radiometer is

$$
\left(\frac{E}{N_0}\right)_{recv} = \sum_{j=1}^{U} \frac{E_j}{N_0} = \sum_{j=1}^{U} T_1 \tau_j \, \frac{S_C}{N_0} \left(\frac{R_{Cj}}{R_{Ij}}\right)^2 \tag{3.59}
$$

If the network uses FDMA, and each emitter has a 100% duty cycle ($\tau_j = 1$), then

$$
\left(\frac{E}{N_0}\right)_{FDMA} = T_1 \, \frac{S_C}{N_0} \sum_{j=1}^{U} \left(\frac{R_{Cj}}{R_{Ij}}\right)^2 \tag{3.60}
$$

Conversely, for a TDMA network in which each user fills its entire time slot, the duty cycle of each waveform as observed by the radiometer is $\tau_j = T_2/T_1 = 1/M$. Furthermore, each user's data rate must increase by a factor of M to account for the limited access to the channel, i.e., $R_b' = M R_b$. Therefore, the increase in required signal power to support the higher data rate is offset by an equivalent reduction in signal duration—which means the received energy-to-noise ratio from each user in the TDMA network is the same as for FDMA, and the two networks offer the same detectability:

$$
\left(\frac{E}{N_0}\right)_{TDMA} = T_1 \left(M \frac{S_C}{N_0}\right) \sum_{j=1}^{U} \frac{1}{M} \left(\frac{R_{Cj}}{R_{Ij}}\right)^2 \tag{3.61}
$$

$$
= \left(\frac{E}{N_0}\right)_{FDMA} \tag{3.62}
$$

Now consider the filter bank and time slot detectors. For both detectors, the overall P_F and P_D are

$$
\begin{aligned}
P_F \;&= 1 - (1 - Q_F)^M \\
P_D \;&= 1 - (1 - Q_F)^{M-U} \prod_{j=1}^{U} (1 - Q_{Dj})
\end{aligned}
$$

The channel/time slot false alarm probability is $Q_F = 1 - (1 - P_F)^{1/M}$. The channel probability of detection for the filter bank detector is

$$
Q_{Dj} = Q \left[Q^{-1}(Q_F) - \frac{E_j/N_0}{\sqrt{T_1 W_2}} \right] \quad \text{FB detector} \tag{3.63}
$$

while the time slot detection probability is

$$Q_{Dj} = Q\left[Q^{-1}(Q_F) - \frac{E_j/N_0}{\sqrt{T_2 W_1}}\right] \quad \text{TS detector} \tag{3.64}$$

It was just shown that E_j/N_0 is independent of whether the signals are divided into frequency channels or time slots. Because $T_1 W_2 = T_2 W_1 = T_1 W_1/M$, it is clear that Equations (3.63) and (3.64) are equivalent, and the two detectors yield identical performance.

The duality between FDMA and TDMA is easily demonstrated for the stand-off intercept model as well. From Table 3.3, the filter bank detector quality factor is

$$Q_{FB} = \frac{[Q^{-1}(Q_F) - Q^{-1}(Q_D)]\sqrt{W_2/T_1}}{R_b(E_b/N_0)} \frac{1}{G_I} \tag{3.65}$$

and for the time slot detector,

$$Q_{TS} = \frac{[Q^{-1}(Q_F) - Q^{-1}(Q_D)]\sqrt{W_1/T_2}}{M R_b(E_b/N_0)} \frac{1}{G_I} \tag{3.66}$$

But the values of Q_F and Q_D are the same for both detectors, since they depend solely on M, P_D, and P_F. Taking the ratio of the two quality factors yields

$$\frac{Q_{TS}}{Q_{FB}} = \frac{1}{M} \frac{\sqrt{W_1/T_2}}{\sqrt{W_2/T_1}} = \frac{1}{M} \frac{\sqrt{M W_2/T_2}}{\sqrt{W_2/M T_2}} = 1 \tag{3.67}$$

Chapter 4

LPI Network Waveform Design Considerations

4.1   Motivation

Two intercept models for determining the detectability of multiple access LPI networks were developed in Chapter 3. In the dispersed network intercept model, the network users are geographically dispersed, and the detectability calculations involve computing the probability of detection based on the energy received from each emitter at the intercept receiver. Unfortunately, these calculations are tedious and highly scenario-dependent. A change in any network parameter (such as a transmitter location, signal bandwidth, etc.), requires recomputation of entire received energy surface (Figure 3.3).

The stand-off network intercept model was developed to deemphasize the scenario-dependent factors, such as transmitter placement, and focus on how the waveforms affect network detectability. In this model, it is assumed that the network emitters are close together and have equal power levels, hence equal energy is received from each transmitter. Network LPI quality factors, summarized in Table 3.3, were then developed to illustrate the relationship among the intercept and communication ranges, transmitted waveform parameters, and communication and intercept receiver performance.

In this chapter, these network LPI quality factors will be used to provide insight into the design of effective network waveforms for the stand-off intercept scenario. Because the mobility and connectivity requirements of the tactical LPI network often lead to the use of omnidirectional antennas, effective waveform design is critical to improving the covertness of the network.

73

Ideally, it would be desirable to determine the "best" multiple access waveform for LPI purposes, but this would be extremely tedious and time consuming, especially for the dispersed network intercept model with its dependence on transmitter placement. Economic and practical constraints must also be considered. For example, the FDMA and TDMA network schemes are somewhat limited in providing covert communications, while the FH-CDMA network scheme, on the other hand, is much more useful for LPI purposes, as illustrated in the examples in Section 3.6.

Advantages of the FH-CDMA network include the ability to let each user access an extremely wide bandwidth via frequency hopping, thereby improving the LPI and AJ properties of the individual. The operating bandwidth need not be coherent, due to the ability to use orthogonal waveforms which can be detected noncoherently, such as FSK and cyclic code shift keying (CCSK). Furthermore, the FH-CDMA waveforms offer a great degree of flexibility in waveform design to improve LPI performance, such as data rate adaptation via pulse combining, and varying the hop rate to defeat the FB/BMW detector.

In this chapter, emphasis will be placed on the detectability of the FH-CDMA network scheme, and how its waveforms can be structured to provide improved LPI performance. The techniques presented here could also be applied to other network schemes, such as FDMA, TDMA, and the Joint Tactical Information Distribution System (JTIDS), which is somewhat of a hybrid between TDMA and FH-CDMA. Although the network LPI quality factors were developed for the stand-off interception scenario, the results of this chapter will also apply to the dispersed network, since any action which makes a single emitter more covert will improve the covertness of the overall network.

4.1.1 Link Waveform Design

As discussed in Chapter 2, waveform design techniques for the simple LPI link are easily evaluated using the concept of the modulation quality factor, defined as follows,

$$Q_{MOD} = \frac{S_I/N_0}{S_C/N_0} \tag{4.1}$$

where S_I/N_0 and S_C/N_0 are the signal-to-noise ratios at the intercept and communications receivers, required to achieve their respective performance levels.

The modulation quality factor is an effective waveform design tool since it ignores all *scenario dependent* factors (such as antennas and atmospheric effects)—only the parameters of the waveform (i.e., modulation, hop rates, bandwidth) and the detection methods (i.e., noncoherent or coherent) are important. Any action which increases S_I/N_0 or decreases S_C/N_0 will increase Q_{MOD} and therefore improve covertness.

S_I/N_0 is primarily a function of the interceptor's desired performance (P_D and P_F), bandwidth, and observation time, which are usually matched to those of the signal. Effective LPI waveforms generally use time hopping and frequency spreading to increase S_I/N_0, thereby increasing Q_{MOD}. Adjusting the hop rate is also an effective technique for defeating channelized receivers, such as the FB/BMW detector. S_C/N_0 depends on the desired communication bit error probability and the data rate. Common techniques for reducing S_C/N_0 include the use of energy-efficient M-ary waveforms which require less E_b/N_0 for a given P_E, error control coding, and data rate control.

4.1.2 Extension to LPI Networks

The LPI network is essentially a collection of interconnected links, so these same waveform design techniques apply to LPI networks as well. Any action which reduces the detectability of a single network node inherently reduces the detectability of the network. Hence, low data rate waveforms using higher order modulation schemes and coding should be used to reduce the required transmit power levels. Furthermore, the waveforms should have large time-bandwidth products to reduce detectability by an unintended listener.

There are two fundamental differences between the design of waveforms for simple LPI links and multiple access networks, however. First, from the communications perspective, all waveforms used within the network must be compatible with the given multiple access scheme. In other words, the network users cannot arbitrarily adapt their waveforms to improve LPI in a manner which would disrupt the other network users. For example, when using FH-CDMA, users must not deviate from their assigned hop patterns and channel assignments, nor can their hop rates change independently. Section 4.2 addresses the reduction of S_C/N_0 through modulation, coding, and data rate control techniques, which are applicable to multiple access networks.

Second, the interceptor receives energy from multiple sources, so when more emitters are added, the network becomes less covert. However, the two receivers studied in this chapter (wideband radiometer and FB/BMW detector) process the energy differently, as is evident in their network LPI quality factors. From Section 3.2, the radiometer's quality factor is [1]

$$Q_{RAD} = \left(\frac{R_C}{R_{RAD}}\right)^2 = \frac{(S_I/N_0)_{RAD}}{(S_C/N_0)} \frac{1}{UG_I} \tag{4.2}$$

where R_{RAD} is the radiometer detection range, and

$$\left(\frac{S_I}{N_0}\right)_{RAD} \approx \left[Q^{-1}(P_F) - Q^{-1}(P_D)\right] \sqrt{\frac{W_1}{T_1}} \qquad T_1 W_1 \geq 1000 \tag{4.3}$$

From Section 3.5, the FB/BMW detector quality factor is

$$Q_{FB} = \left(\frac{R_C}{R_{FB}}\right)^2 = \frac{(S_I/N_0)_{FB}}{(S_C/N_0)} \frac{1}{G_I} \tag{4.4}$$

where R_{FB} is the FB/BMW detection range, and

$$\left(\frac{S_I}{N_0}\right)_{FB} \approx \left[Q^{-1}(Q_F) - Q^{-1}(Q_D)\right] \sqrt{\frac{W_2}{T_2}} \qquad W_2 T_2 \geq 1000 \tag{4.5}$$

The probabilities Q_F and Q_D depend on the number of frequency channels, M, the number of hops observed, N, and the number of active transmitters, U. Obviously, the two detectors will exhibit different sensitivities to changes in these waveform parameters. These issues are developed in Section 4.3.

4.2 Modulation and Coding Parameters

The communication receiver's SNR depends on the desired performance (bit error probability) and the modulation scheme, as shown below,

$$\frac{S_C}{N_0} = \zeta_C(P_E) R_b = \left(\frac{E_b}{N_0}\right) R_b \tag{4.6}$$

where E_b/N_0 is the required bit energy-to-noise PSD required to achieve the specified P_E, and R_b is the burst data rate. Three methods for reducing S_C/N_0 will be investigated in this section: energy-efficient modulation, error control coding, and data rate control.

---

[1] For the remainder of this chapter, 100% duty cycle signals will be used ($\tau = 1$)

4.2.1 Higher Order Modulation

Energy efficient, higher order modulation schemes are preferable in LPI communications, since they reduce the SNR per bit, E_b/N_0, required at the demodulator to achieve the desired bit error probability, P_E. As shown in Figure 4.1, M-ary schemes such as FSK and CCSK are much more efficient (in terms of required SNR) than BPSK. This was observed from the sample detection scenarios in Chapter 3, in which networks using FH-CDMA with 32-ary FSK/CCSK were less detectable than DS-CDMA networks.
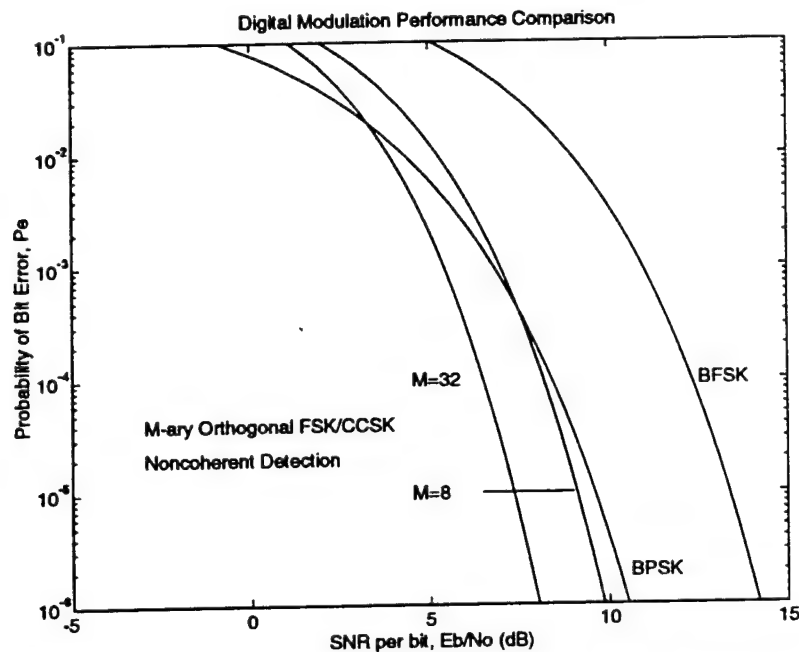
Figure 4.1: Comparison of Various Digital Modulation Schemes

Subsequent analyses will focus on the FH-CDMA network using M-ary orthogonal waveforms, because of their energy efficiency. Although coherent detection is generally superior to noncoherent detection, it is in practice difficult to maintain the necessary phase coherence while synthesizing the hop frequencies. The extremely wide spread spectrum bandwidths may also preclude the use of coherent waveforms.

The network LPI quality factors for a stand-off intercept scenario using the wideband radiometer and FB/BMW detectors are given in Table 3.3. For both detectors, reducing E_b/N_0 increases the Q_{MOD} and Q_{LPIN}. Because of the $1/R^2$ propagation, any reduction

in the required E_b/N_0 by a factor of, say Δ_E, will allow the network transmitters to either maintain their current power levels and extend their broadcast ranges by $\sqrt{\Delta_E}$, or reduce power by Δ_E, forcing the interceptor to close its distance by a factor of $\sqrt{\Delta_E}$.

Theoretically, the size of the M-ary alphabet should be as large as possible, although very large alphabets become impractical. As shown in Figure 4.2, increasing M from 2 to 32 results in a substantial decrease in E_b/N_0 by about 6 dB for $P_E = 10^{-5}$. For very large M, however, a point of diminishing returns is reached, and the additional cost and complexity must be considered. For example, increasing M from 32 to 1024 squares the number of frequency cells which must be detected, yet the required SNR is reduced only by 1.5 dB.
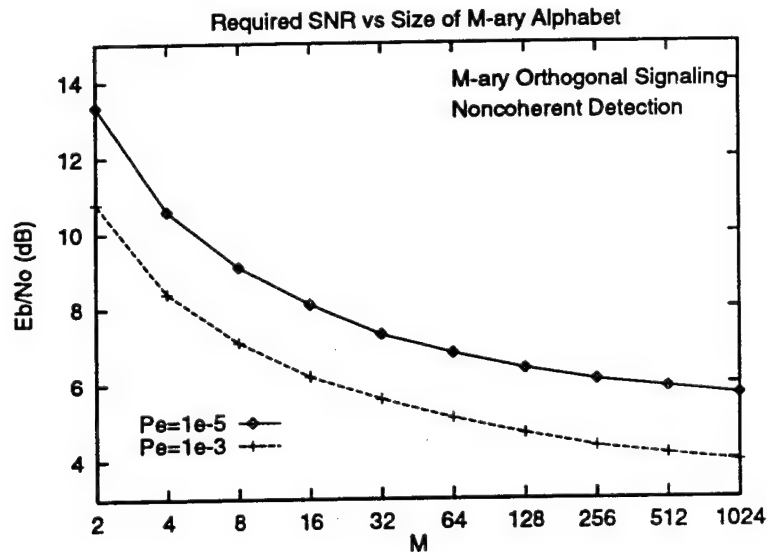
Figure 4.2: Required E_b/N_0 for M-ary Modulation

4.2.2　Error Control Coding

Error control coding can be used to effectively reduce the E_b/N_0 required at the LPI communications receiver to obtain the desired bit error probability. By adding a degree of redundancy into the transmitted data, some error patterns can be detected and corrected at the communication receiver.

Although there are many coding schemes, the nonbinary Reed-Solomon codes will be considered here, because they are well suited for use in conjunction with M-ary modulation. Because of their large distance properties, they are also effective for correcting burst errors, possibly due to pulse jamming. An (N, K) Reed-Solomon code is described as follows:

$$
\begin{aligned}
N &= q - 1 = 2^k - 1 \\
K &= 1, 2, \ldots, N - 1 \\
d_{min} &= N - K + 1
\end{aligned}
$$

where K is the number of data symbols being encoded, N is the number of symbols in an encoded block (or code word), and d_{min} is the minimum distance between valid code words. The (N, K) code can correct errors with up to $t = (d_{min} - 1)/2 = (N - K)/2$ symbols. The code rate is defined as $r_c = K/N$.

The Reed-Solomon encoder maps a K-tuple of nonbinary symbols into an N-tuple code word, where each symbol is selected from an alphabet of $q = 2^k$ symbols—each symbol represents k bits of information. If the code is used in conjunction with M-ary orthogonal signaling with $M = q = 2^k$, then each of the q symbols is matched to a corresponding transmission waveform. The transmission of an entire N-tuple code word is therefore achieved by sending N waveforms, where each waveform comes from the M-ary signal set (i.e., FSK tones).

For a symmetric memoryless channel with M inputs and outputs (a generalization of the binary symmetric channel), the probability that a received code word cannot be properly decoded is upper bounded by the probability that more than t code word symbols were in error:

$$
P_{CE} \leq \sum_{i=t+1}^{N} \binom{N}{i} P_M^i (1 - P_M)^{N-i} \tag{4.7}
$$

where P_M is the channel symbol error probability for the transmitted code word symbols. For M-ary orthogonal signaling with noncoherent detection,

$$
P_M = \frac{e^{-\gamma}}{M} \sum_{n=2}^{M} \binom{M}{n} (-1)^n e^{\gamma/n} \tag{4.8}
$$

where $\gamma = r_c \log_2 M (E_b/N_0)$ is the SNR per coded symbol.

If a received code word is in error, the probability of error for a single code word symbol is

$$P_{SE} = \sum_{i=t+1}^{N} \left(\frac{i}{N}\right) \binom{N}{i} P_M^i (1 - P_M)^{N-i} \tag{4.9}$$

Figure 4.3 illustrates the improvements in E_b/N_0 gained through the use of Reed-Solomon coding in conjunction with 32-ary orthogonal signaling. These curves were generated by substituting (4.8) into (4.9) and converting the symbol error probability to bit error probability as follows,

$$P_E = P_{SE} \frac{M/2}{M-1} \tag{4.10}$$

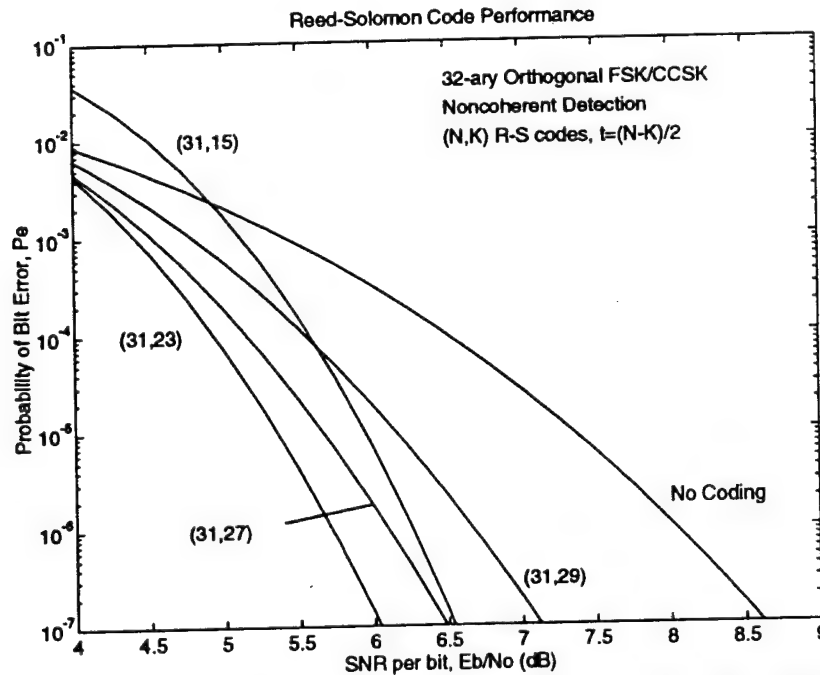Figure 4.3: Comparison of Various Reed-Solomon Codes using 32-ary Modulation

Modifying Equation (4.6) to include the effects of coding yields

$$\frac{S_C}{N_0} = \left(\frac{E_b}{N_0}\right)_1 \frac{R_b}{G_{code}} \tag{4.11}$$

where $(E_b/N_0)_1$ is the required SNR per uncoded bit, and R_b is the data rate for information and coding overhead bits. G_{code} is the *coding gain*, which when expressed

in dB, is the distance between the uncoded and coded bit error probability curves for a specified P_E. G_{code} depends on a number of factors, such as the modulation, noise characteristics, the code properties, and the P_E at which it is measured, as illustrated in Figure 4.4. It is possible that $G_{code} < 0$ dB, in which case the error correcting capability of the code is overcome by the increased overhead, and use of the code actually degrades performance.
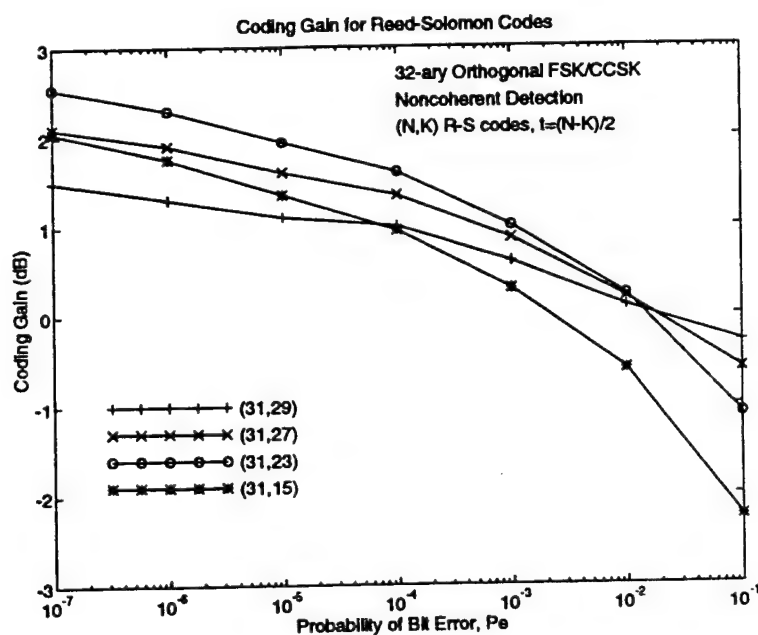
Figure 4.4: Coding Gain for Reed-Solomon Codes

4.2.3 Data Rate Reduction

Data Compression

Almost all types of raw digital data, whether generated by computer or quantized from analog sources, contain redundant information. Transmission of the raw data is therefore wasteful, since the total number of transmitted bits is higher than actually necessary. The purpose of data compression, also known as source coding, is to reduce the amount of information (by eliminating redundant data) before transmission over the communication channel. In situations where limited-capacity channels are available,

data compression is often a necessity. Note that data compression should precede error control coding.

A number of compression algorithms have been developed to exploit redundancies found in various types of data (speech, data, graphics, and video). An excellent overview of data compression and its application to LPI system design is provided in [0]. Some of the more common compression techniques for voice and data are summarized in the following paragraphs.

Voice Data. Voice coders fall into three categories: waveform coding, source modeling, and hybrids. Waveform coders simply map the speech waveform onto a second waveform. Common examples include pulse code modulation (PCM), continuously variable slope delta modulation (CVSD), and adaptive predictive coding (APC).

Source modeling algorithms include linear predictive coding (LPC), in which the vocal tract is modeled by a linear time-varying filter, and format trackers which track the resonances of the vocal tract. Hybrid coding algorithms use a combination of waveform coding and source modeling; examples are multipulse LPC and residual excited linear prediction (RELP).

Further data rate reductions may be obtained using vector quantization (VQ), frame repeat VQ (FRVQ), and matrix quantization (MQ). Word recognition techniques can provide very high compression ratios, at the expense of linguistic and vocabulary constraints. The performance of several common voice coding algorithms are summarized in Table 4.1 (from [0]). The Diagnostic Rhyme Test (DRT) is used as the primary measure of intelligibility—i.e., can the listener understand the message? Table 4.2 (also from [0]) gives a subjective relationship between DRT scores and speech quality.

Digital Data. Computer generated data, such as radar target reports, teletype text, graphics (including facsimile), and database information can also be compressed to reduce the amount of raw data overhead. Unlike voice coding, however, compression of digital data must be *lossless*—the receiver must be able to recover the data on an exact bit-by-bit basis. Some common lossless compression techniques include the following:

- Run-length encoding — streams of identical characters are replaced with a flag, the character itself, and the number of times that character is repeated

- Half-byte encoding — characters are grouped based on a defined character set

definition (i.e., the digits 0-9 have ASCII representations which begin with 011, so the last four bits uniquely identify the digits)

- Diatomic compression — characters are compressed in pairs

- Pattern matching — common character groups or strings (such as computer source program keywords) are identified by a unique codeword

- Statistical compression — variable length codewords are assigned based on the relative frequency of the data (i.e., Shannon-Fano and Huffman coding)

The reduction in S_C/N_0 due to data compression is the compression ratio, defined as $C = R_b/R_c$ where R_b and R_c are the raw and compressed bit rates, respectively. If the transmitter reduces its power by C, then the interceptor's detection range decreases by $\sqrt{C}$. Conversely, if the transmitter maintains its current power level, the communication range can be extended by $\sqrt{C}$.

Speech Coding Algorithm	Data Rate (bps)	Tolerable Error Rate	Complexity	Performance (DRT)
PCM	64000	>10%	Simple	Mid-High 90s
CVSD	16000	10%	Simple	Mid 90s
APC	9600	5%	Moderate	Upper 80s
MLPC, RELP	5000	5%	Moderate	Upper 80s
LPC-10	2400	1-2%	Moderate	Mid-High 80s
VQ w/LPC	800	0.5-1%	Mod-High	Low-Mid 80s
Format Tracker	600	0.5-1%	High	High 70s to Low 80s
FRVQ w/LPC	400	0.1-0.5%	Moderate to High	Mid 70s
MQ w/LPC	300	0.1-0.5%	High	Mid 70s
Word Recog	20-200	-	High	-

Table 4.1: Comparison of Speech Compression Algorithms

DRT Range	Voice Intelligibility
96-100	Excellent
91-96	Very Good
87-91	Good
83-87	Moderate
79-83	Fair
75-79	Poor
70-75	Very Poor
<70	Unacceptable

Table 4.2: Interpretation of Diagnostic Rhyme Test (DRT) Intelligibility Scores

Reducing the Signaling Rate

Perhaps the simplest way to reduce the data rate is to extend the symbol duration of the signals which are applied to the channel. For example, if one M-ary symbol is transmitted each hop period, the data rate is $R_b = \log_2 M/T_h$ bps. If the hop rate is reduced (T_h is increased), then R_b decreases as well. This scheme does have some disadvantages. First, the signal features would change, which could be exploited by the interceptor—for example, decreasing the hop rate typically favors the FB/BMW detector, as will be shown in a later section. Second, and more importantly, any changes in the hop rate must be coordinated among all network users—individual users cannot adjust their hop rates arbitrarily.

Pulse Combining

An alternative to slowing down the signaling rate is pulse combining, in which multiple hops are used to transmit a single data symbol, as shown in Figure 4.5. This method of network data rate control is superior to simply slowing down the signals, since the hop rate need not change—hence it can be applied on an individual basis. Covertness is improved, since the required SNR per pulse decreases as more pulses are integrated, allowing a reduction in transmitter power. Furthermore, the transmitted signal features are unchanged, and the intercept receiver would be unaware that pulse combining is being used. In other words, pulse combining can be used in conjunction with increasing the hop rate (to defeat the FB/BMW detector) while maintaining a constant data rate
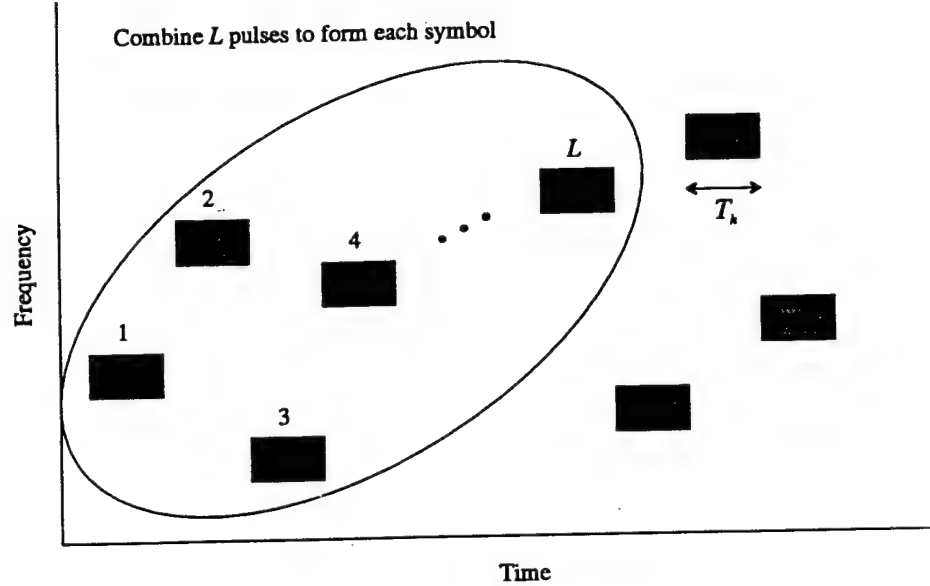
(to maintain covertness).

Figure 4.5: Pulse Combining

Noncoherent pulse combining is conceptually quite similar to multichannel diversity signaling, which is developed in [0]. However, there is an error in Proakis' Equation (4.4.22), which gives the symbol error probability with L-channel combining. With this in mind, the probability of error will be derived in the following paragraphs; for the most part, the development follows that given by Proakis.

First, using M-ary orthogonal signaling, noncoherent detection, and L-pulse combining, the transmitted waveforms can be expressed as follows:

$$s_{nm}(t) = \text{Re}\left[u_{nm}(t)e^{j2\pi f_c t}\right] \qquad \begin{aligned} 0 &\leq t \leq T \\ n &= 1, 2, \ldots, L \\ m &= 1, 2, \ldots, M \end{aligned} \qquad (4.12)$$

where $u_{nm}(t)$ is the equivalent low pass waveform, M is the size of the symbol set, and L is the number of pulses to be combined. The pulses have equal energy, with

$$E = \frac{1}{2}\int_0^T u_{nm}(t)u_{nm}^*(t)\, dt \qquad \begin{aligned} n &= 1, 2, \ldots, L \\ m &= 1, 2, \ldots, M \end{aligned} \qquad (4.13)$$

The waveforms $\{s_{nm}(t)\}$ transmitted over the L time slots (channels) are scaled and phase-shifted by the factors $\{\alpha_n\}$ and $\{\phi_n\}$. For simplicity, it will be assumed here that the channel attenuations are identical, i.e., $\alpha_n = \alpha$. Furthermore, since the signals are detected noncoherently, the phase terms have no effect on the receiver performance, and can be ignored. Denoting $z_n(t)$ as the additive white Gaussian noise present in each pulse interval, the received equivalent low pass signals for the L pulses are

$$r_n(t) = \alpha u_{nm}(t) + z_n(t) \qquad \begin{array}{l} 0 \le t \le T \\ n = 1, 2, \ldots, L \\ m = 1, 2, \ldots, M \end{array} \qquad (4.14)$$

Since the pulses do not overlap, the noise processes $\{z_n(t)\}$ are assumed to be statistically independent, identically distributed Gaussian processes. A noncoherent square-law detector produces the following decision variables,

$$
\begin{aligned}
U_m &= \sum_{n=1}^{L} \left| \int_0^T r_n(t) u_{nm}^*(t) \, dt \right|^2 \\
&= \sum_{n=1}^{L} \left| \int_0^T \left[\alpha u_{nm}(t) + z_n(t) \right] u_{nm}^*(t) \, dt \right|^2 \\
&= \sum_{n=1}^{L} \left| \alpha \int_0^T u_{nm}(t) u_{nm}^*(t) \, dt + \int_0^T z_n(t) u_{nm}^*(t) \, dt \right|^2 \qquad (4.15) \\
&= \sum_{n=1}^{L} |2E\alpha + N_{nm}|^2 \qquad m = 1, 2, \ldots, M \qquad (4.16)
\end{aligned}
$$

where the $\{N_{nm}\}$ are complex-valued zero-mean Gaussian random variables with variance $\sigma^2 = 2EN_0$ [0].

If the symbols are equally likely, then the probability of error can be found using just one of the M symbols. For $m = 1$, the signals $u_{n1}(t)$ are sent using L-pulse diversity, and the decision variables of interest are

$$
\begin{aligned}
U_1 &= \sum_{n=1}^{L} |2E\alpha + N_{n1}|^2 \\
U_m &= \sum_{n=1}^{L} |N_{nm}|^2 \qquad m = 2, 3, \ldots, M \qquad (4.17)
\end{aligned}
$$

Since the $\{N_{nm}\}$ are uncorrelated Gaussian random variables, these $\{U_m\}$ are chi-square random variables with $2L$ degrees of freedom. They are statistically independent, and

have the following probability density function:

$$f(u_m) = \frac{1}{\sigma^{2L} \, 2^L \, \Gamma(L)} \, u_m^{L-1} e^{-u_m/2\sigma^2} \qquad \begin{matrix} u_m & \geq 0 \\ m & = 2, 3, \ldots, M \end{matrix} \qquad (4.18)$$

Likewise, U_1 is a noncentral chi-square random variable, with $2L$ degrees of freedom and noncentrality parameter,

$$\lambda = \sum_{n=1}^{L} (2E\alpha)^2 = 4LE^2\alpha^2 \qquad (4.19)$$

Its probability density function is therefore

$$f(u_1) = \frac{1}{2\sigma^2} \left(\frac{u_1}{\lambda}\right)^{\frac{L-1}{2}} e^{-(u_1+\lambda)/2\sigma^2} I_{L-1}\left(\frac{\sqrt{u_1\lambda}}{\sigma^2}\right) \qquad u_1 \geq 0 \qquad (4.20)$$

where $I_n(x)$ is the nth order modified Bessel function of the first kind.

The channel probability of symbol error, P_M, is the probability that one or more decision variables $\{U_m\}$, $m = 2, 3, \ldots, M$, is greater than U_1. Alternatively, P_M can be determined using the complement of a correct decision:

$$\begin{aligned} P_M &= 1 - \Pr\left(U_2 < U_1, U_3 < U_1, \ldots, U_M < U_1\right) \\ &= 1 - \int_0^\infty \left[\Pr(U_2 < u_1 | U_1 = u_1)\right]^{M-1} f(u_1) \, du_1 \end{aligned} \qquad (4.21)$$

where

$$\Pr(U_2 < u_1 | U_1 = u_1) = \int_0^{u_1} f(u_2) \, du_2 \qquad (4.22)$$

and $f(u_2)$ is given in (4.18). This integral can be evaluated in closed form by first expressing it in the form of the incomplete gamma function, and then integrating by parts [0], resulting in

$$\Pr(U_2 < u_1 | U_1 = u_1) = 1 - e^{-u_1/2\sigma^2} \sum_{k=0}^{L-1} \frac{(u_1/2\sigma^2)^k}{k!} \qquad (4.23)$$

Substituting (4.20) and (4.23) into (4.21),

$$\begin{aligned} P_M &= 1 - \int_0^\infty \left[1 - e^{-u_1/2\sigma^2} \sum_{k=0}^{L-1} \frac{(u_1/2\sigma^2)^k}{k!}\right]^{M-1} f(u_1) \, du_1 \\ &= 1 - \int_0^\infty \left[1 - e^{-u_1/2\sigma^2} \sum_{k=0}^{L-1} \frac{(u_1/2\sigma^2)^k}{k!}\right]^{M-1} \\ &\qquad\qquad \frac{1}{2\sigma^2} \left(\frac{u_1}{\lambda}\right)^{\frac{L-1}{2}} e^{-(u_1+\lambda)/2\sigma^2} I_{L-1}\left(\frac{\sqrt{u_1\lambda}}{\sigma^2}\right) \, du_1 \end{aligned} \qquad (4.24)$$

Using a variable substitution of $u_1 = 2\sigma^2\nu$, $du_1 = 2\sigma^2\ d\nu$, this simplifies to

$$P_M = 1 - \int_0^\infty \left[1 - e^{-\nu} \sum_{k=0}^{L-1} \frac{\nu^k}{k!} \right]^{M-1} \left(\frac{2\sigma^2\nu}{\lambda} \right)^{\frac{L-1}{2}} e^{-(\nu+\lambda/2\sigma^2)} I_{L-1} \left(\sqrt{\frac{2\nu\lambda}{\sigma^2}} \right)\ d\nu \quad (4.25)$$

Substituting $\lambda = 4LE^2\alpha^2$ and $\sigma^2 = 2EN_0$,

$$P_M = 1 - \int_0^\infty \left[1 - e^{-\nu} \sum_{k=0}^{L-1} \frac{\nu^k}{k!} \right]^{M-1} \left(\frac{N_0\nu}{LE\alpha^2} \right)^{\frac{L-1}{2}} e^{-\nu-LE\alpha^2/N_0} I_{L-1} \left(2\sqrt{\frac{\nu LE\alpha^2}{N_0}} \right)\ d\nu$$
$$(4.26)$$

It is now recognized that $LE\alpha^2/N_0$ is the total received symbol SNR which has been split evenly among L channels (pulses). Letting $\gamma = LE\alpha^2/N_0 = \log_2 M(E_b/N_0)$, the probability of symbol error is

$$P_M = 1 - \int_0^\infty \left[1 - e^{-\nu} \sum_{k=0}^{L-1} \frac{\nu^k}{k!} \right]^{M-1} \left(\frac{\nu}{\gamma} \right)^{\frac{L-1}{2}} e^{-(\nu+\gamma)} I_{L-1} \left(2\sqrt{\nu\gamma} \right)\ d\nu \quad (4.27)$$

The above equation can be used to determine P_M; a final variable substitution, $\nu = \gamma x$, could also be used:

$$P_M = 1 - \int_0^\infty \left[1 - e^{-\gamma x} \sum_{k=0}^{L-1} \frac{(\gamma x)^k}{k!} \right]^{M-1} \gamma\ x^{\frac{L-1}{2}} e^{-\gamma(x+1)} I_{L-1} \left(2\gamma\sqrt{x} \right)\ dx \quad (4.28)$$

For orthogonal M-ary signalling, the relationship between the bit and symbol error probabilities is

$$P_E = P_M \frac{M/2}{M-1} \quad (4.29)$$

Equations (4.27) and (4.28) must be solved numerically, with γ, L, and M as input parameters. For small values of M, a union bound can be formed as $P_M < (M-1)\,P_2(L)$, where $P_2(L)$ is the probability of error in choosing between U_1 and any of the other $M - 1$ variables [0]:

$$P_2(L) = \frac{1}{2^{2L-1}} e^{-k\gamma_b/2} \sum_{n=0}^{L-1} c_n \left(\frac{k\gamma_b}{2} \right)^n \quad (4.30)$$

where $\gamma_b = E_b/N_0$, $k = \log_2 M$, and

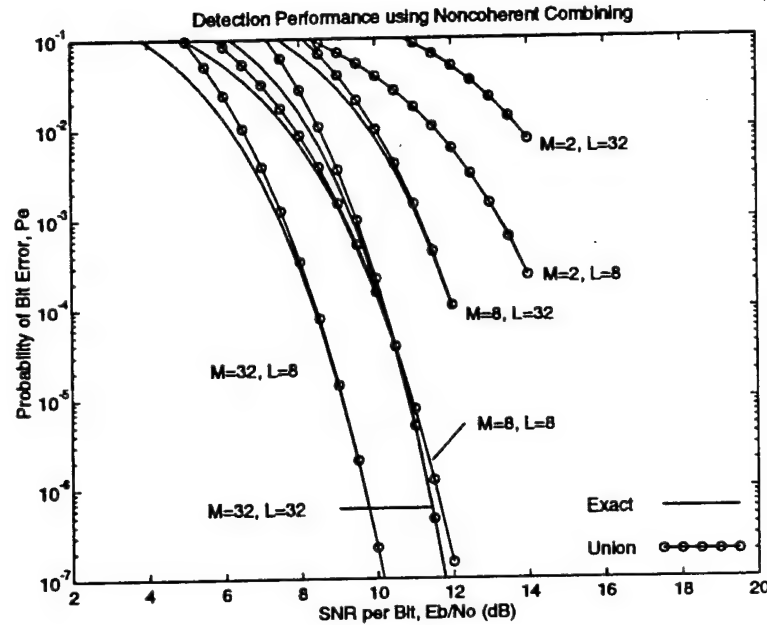$$c_n = \frac{1}{n!} \sum_{j=0}^{L-1-n} \binom{2L-1}{j} \quad (4.31)$$

Figure 4.6: Comparison of Union Bound to Exact Results

Figure 4.6 illustrates the accuracy of the union bound for several values of M and L. For $M = 2$, there is no difference between the approximated and exact results. As M increases, the union bound offers good results only for large signal-to-noise ratios.

It is well known that noncoherent detection and combining is not as efficient as coherent processing, due to *noncoherent combining losses* (also known as integration loss). Let $(E/N_0)_1$ be the SNR of a single pulse which allows detection with a specified probability of error, P_E. If this energy were split equally among L pulses and combined coherently, the required per pulse SNR to achieve the same P_E would be $E_c/N_0 = (E/N_0)_1/L$. If the pulses are combined noncoherently, however, the SNR of each pulse, E_p/N_0, must be greater than E_c/N_0 to obtain the same P_E—hence the total SNR must be greater than $(E/N_0)_1$. This is illustrated in Figure 4.7, which shows the probability of bit error as a function of combining and the SNR per bit ($E_b/N_0 = \gamma/\log_2 M$). As shown, for a constant P_E, the required SNR increases as more pulses are combined.
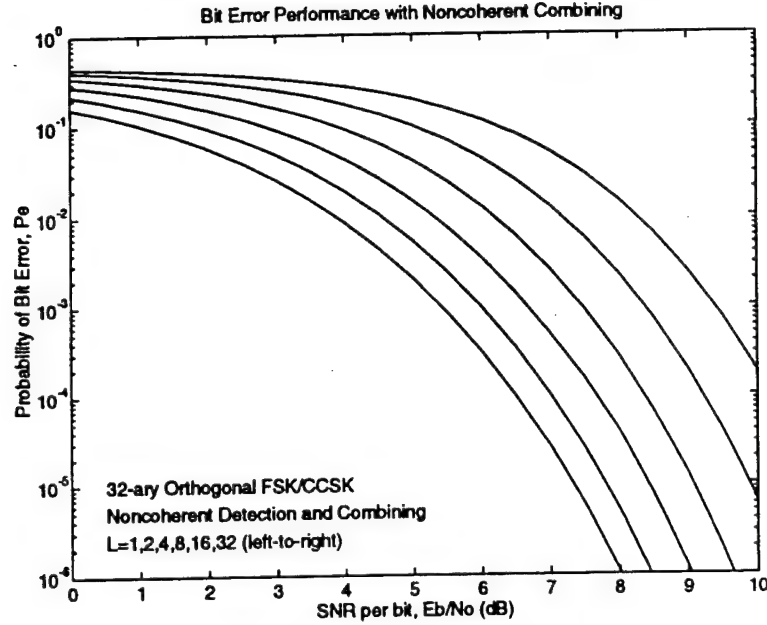
Figure 4.7: Performance Curves for Noncoherent Combining

The noncoherent combining loss is defined as follows:

$$L_C = \frac{E_p/N_0}{E_c/N_0} = \frac{E_p/N_0}{(E/N_0)_1/L} = \frac{(E/N_0)_L}{(E/N_0)_1} \tag{4.32}$$

where $(E/N_0)_1$ is the SNR required for no combining ($L = 1$), and $(E/N_0)_L = LE_p/N_0$ is the post integration SNR of L pulses. L_C is a function of P_E and L, as shown in Figure 4.8; for constant L, L_C decreases as P_E decreases.

In spite of these losses, pulse combining offers a real improvement in covertness. From (4.6), the required communication SNR can be modified to account for pulse combining as shown (without error control coding),

$$\frac{S_C}{N_0} = \left(\frac{E_b}{N_0}\right)_1 \frac{L_C R_b}{L} = \left(\frac{E_b}{N_0}\right)_1 \frac{L_C}{L} \frac{\log_2 M}{T_h} \tag{4.33}$$

where $(E_b/N_0)_1$ and R_b are the required SNR per bit and data rate prior to combining. To obtain a desired data rate of R_d bps, the required level of combining is

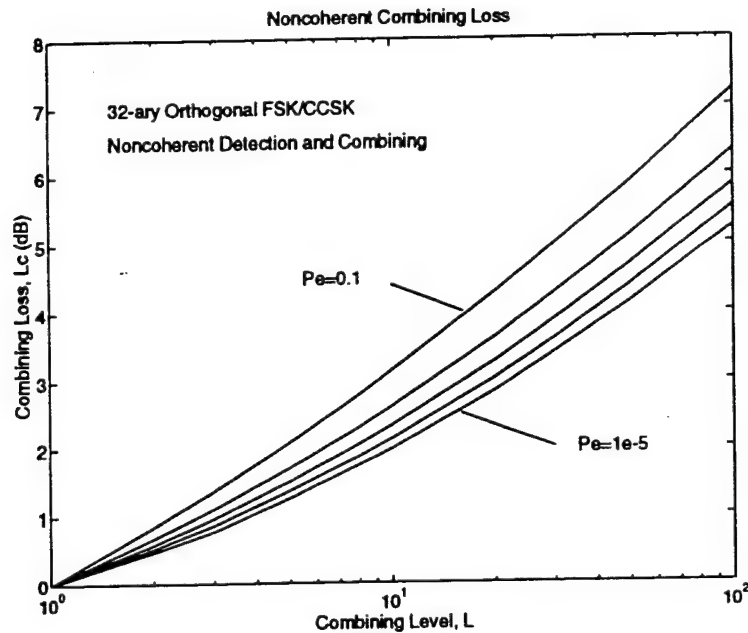$$L = \frac{R_b}{R_d} = \frac{\log_2 M}{T_h R_d} \tag{4.34}$$

Figure 4.8: Noncoherent Combining Loss

The effect of combining on the required SNR is totally embodied in the factor L_C/L, which is plotted in Figure 4.9. The dashed line represents lossless combining, in which case S_C/N_0 decreases by $10\log(L)$ dB. With noncoherent detection and combining, however, an increase in L is offset by a slight increase in L_C, resulting in a change in S_C/N_0 of $10\log(L_C/L)$ dB. With $P_E = 10^{-5}$ and $L = 10$, S_C/N_0 decreases by about 8 dB. If the transmit power is reduced by this amount, the intercept range drops by 4 dB—i.e., if the interceptor were originally 10 miles away, it must close to within 4 miles to maintain the same performance level.

4.2.4 Coding in Conjunction with Pulse Combining

Reed-Solomon coding can be used in conjunction with noncoherent pulse combining to lessen the impact of noncoherent combining losses. The probability of channel symbol error using L-pulse diversity is given in (4.27). Substituting this into (4.9) gives the probability that a symbol in the received N-tuple is in error, which can then be used
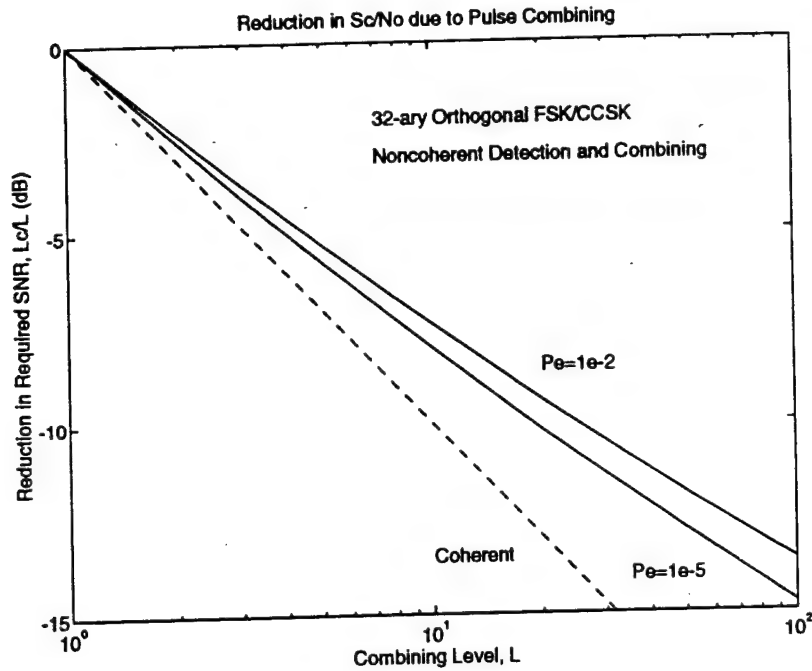
Figure 4.9: Reduction of SNR due to Combining

to compute the bit error probability. Figure 4.10 shows performance curves for $L = 10$ and a $(31, 27)$ code.

The coding gain is a function of the channel symbol error probability, P_M, which depends on L (Equation (4.27)). Therefore, the coding gain is also a function of L, as shown in Figure 4.11. In other words, combining and coding cannot be analyzed independently.

The overall effects of Reed-Solomon coding and noncoherent pulse combining on the required S_C/N_0 can be expressed as follows:

$$\frac{S_C}{N_0} = \left(\frac{E_b}{N_0}\right)_1 R_b \frac{L_C}{L} \frac{1}{G_{code}(L)} \qquad (4.35)$$

where

- $(E_b/N_0)_1$ is the SNR per uncoded/uncombined bit required to obtain the specified P_E

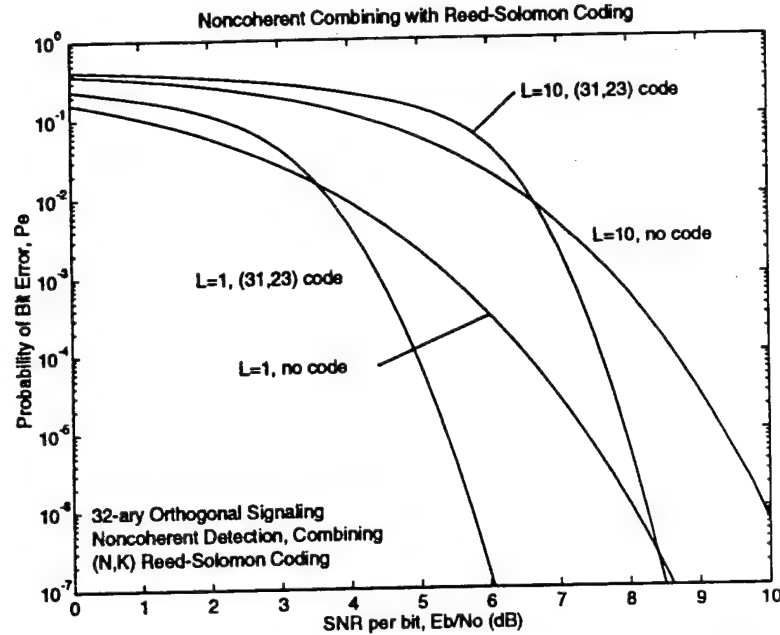- R_b is the burst data rate of the information plus coding overhead

Figure 4.10: Pulse Combining with Reed-Solomon Coding

- L and L_C are the number of pulses combined and the corresponding combining loss

- $G_{code}(L)$ is the coding gain, measured at the specified P_E (a function of L—see Figure 4.11)

4.3 Time-Frequency Parameters

In the previous section, techniques to improve covertness, by increasing the modulation quality factor, focused on the reduction of S_C/N_0. In this section, emphasis is placed on the interceptor's SNR, S_I/N_0. The two intercept receivers considered here are the wideband radiometer and FB/BMW detector.

The required SNRs for the two receivers depend on the desired performance, observation time, and bandwidth, as shown in (4.3) and (4.5). P_F and P_D are *receiver*
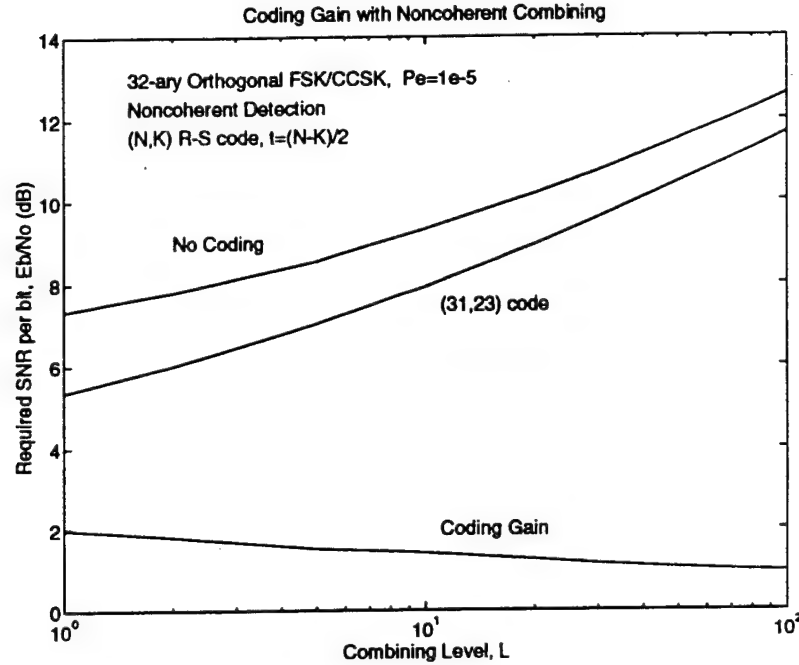
Figure 4.11: Coding Gain as a Function of Combining

parameters controlled by the interceptor; they are usually specified based on the operational mission objectives and other considerations, such as the costs of false alarms and missed detections.

Technically, W_1 and T_1 are receiver parameters as well, since they are ultimately under the control of the interceptor. It is commonly assumed, however, that the interceptor has general knowledge of the signal parameters and therefore sets its bandwidth and observation time accordingly. In this case, W_1 and T_1 essentially become *waveform* parameters which can be adjusted to reduce waveform detectability.

4.3.1 Relative Quality Factor

It is customary to design LPI waveforms such that no one intercept receiver performs substantially better than another. With this in mind, the relative detection range using the FB/BMW compared to the radiometer can be expressed as follows,

$$\left(\frac{R_{FB}}{R_{RAD}}\right)^2 = \frac{Q_{RAD}}{Q_{FB}}$$

$$
\begin{aligned}
&= \frac{(S_I/N_0)_{RAD}/U}{(S_I/N_0)_{FB}} \\
&= \frac{d_R/U\sqrt{W_1/T_1}}{d_F\sqrt{W_2/T_2}}
\end{aligned} \tag{4.36}
$$

where

$$
\begin{aligned}
d_R &= Q^{-1}(P_F) - Q^{-1}(P_D) \\
d_F &= Q^{-1}(Q_F) - Q^{-1}(Q_D)
\end{aligned}
$$

Q_F and Q_D are solved using Table 3.3. The number of hops observed is $N = T_1/T_2$, and if the channels are contiguous, $M = W_1/W_2$. Substituting these into (4.36) yields

$$
\left(\frac{R_{FB}}{R_{RAD}}\right)^2 = \frac{d_R/U\sqrt{W_1/T_1}}{d_F\sqrt{(W_1/M)/(T_1/N)}} \tag{4.37}
$$

$$
= \frac{d_R}{d_F}\frac{1}{U}\sqrt{\frac{M}{N}} \tag{4.38}
$$

Equation (4.38) completely describes the relative performance of the FB/BMW detector compared to the radiometer. For fixed P_F and P_D, the waveform parameters available for optimization are U, M, and N:

- U is the number of active users in the network. U is considered a waveform parameter here since it affects how much energy is dispersed in the overall $W_1 \times T_1$ time-frequency space.

- M is the number of frequency channels, and therefore the maximum number of users allowed at any given time. The network load is therefore defined as U/M. For fixed W_1, increasing M decreases the channel bandwidth.

- N is the number of hops observed. For fixed T_1, varying N has the effect of changing the hop rate: $f_H = 1/T_2 = N/T_1$ hops/sec.

Each of these parameters influences Equation (4.38) in two ways, the obvious one being the factor $(1/U)\sqrt{M/N}$. As shown in Table 3.3, the channel probabilities Q_F and Q_D depend on M, N, and U, as well.

Note that Equation (4.38) only provides information regarding the *relative* performance of the two detectors. For example, the overall bandwidth, W_1, does not appear in the equation, since for a given value of M, any change in W_1 changes W_2 by the same factor. Likewise, for constant N, any change in T_1 results in the same change in T_2.

4.3.2 Frequency Hop Rate

Varying N while keeping T_1 fixed has the effect of changing the hop rate—if $T_1 = 1$ sec, then N is the hop rate. Figures 4.12-4.13 illustrate the effect of N on the relative performance of the two detectors, with M and U as parameters. The general trend is a reduction in FB/BMW detection range, relative to the wideband radiometer, as the hop rate increases. This is consistent with previous research on the interception of single LPI links, and can be attributed to the reduction in integration as the hop rate increases (i.e., consider the effect of decreasing T_2 on Equation (4.5)).

As shown in Figure 4.13, the influence of N diminishes as the load increases. With $U = 10$ and $M = 100$ (10% load), a factor of 10 change in hop rate results in a decrease in relative detection range of 0.8-0.9 dB. For a fully loaded network, changing the hop rate has little or no effect.
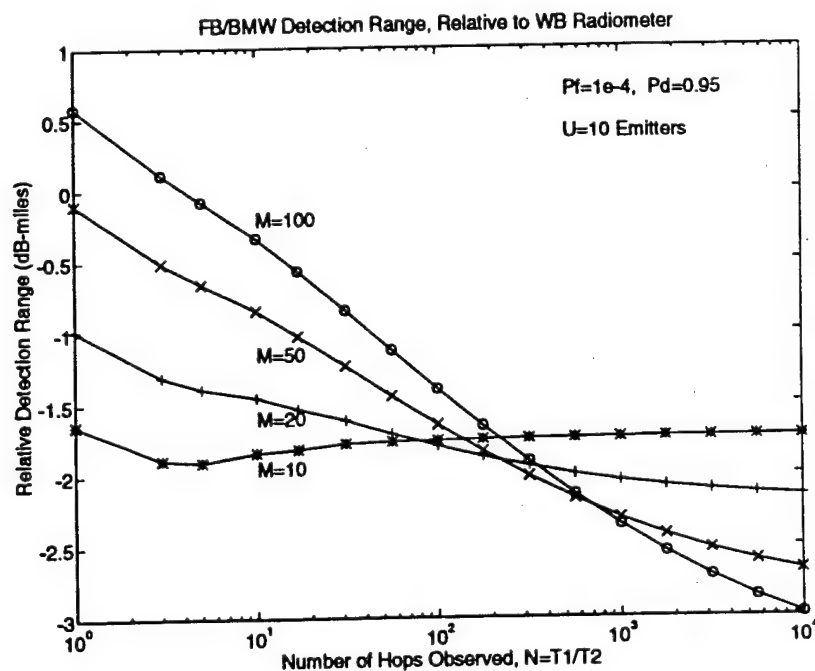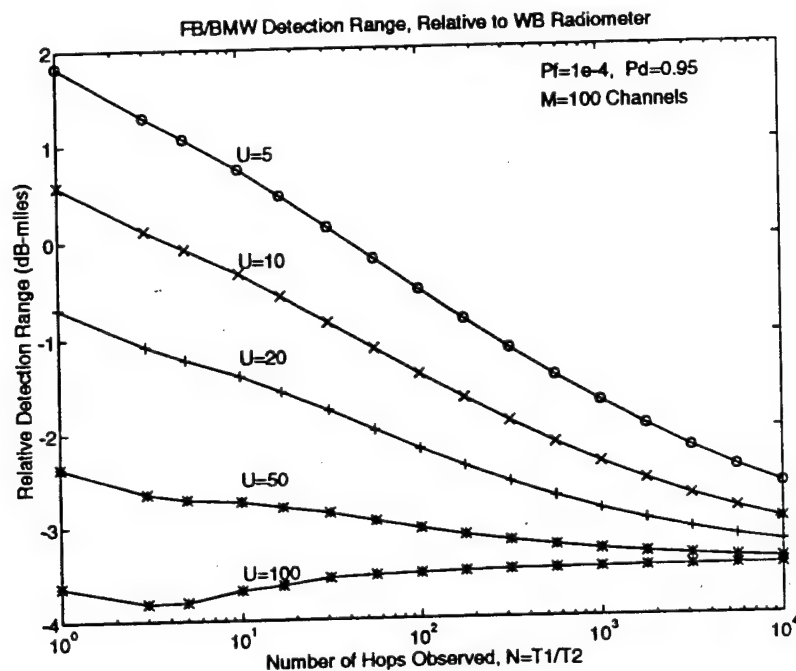

Figure 4.12: Effect of Hop Rate on Detection Range, $U = 10$ Emitters

Figure 4.13: Effect of Hop Rate on Detection Range, $M = 100$ Channels

4.3.3   Number of Channels

When W_1 is fixed, increasing M decreases the channel bandwidth, which reduces the required SNR for the FB/BMW detector. This is illustrated in Figures 4.14-4.15. Increasing M generally favors the FB/BMW detector, although the change becomes less pronounced as the hop rate increases. However, the FB/BMW detector is better than the radiometer (its relative detection range is greater than 0 dB) only when N and U are small, and M is large.
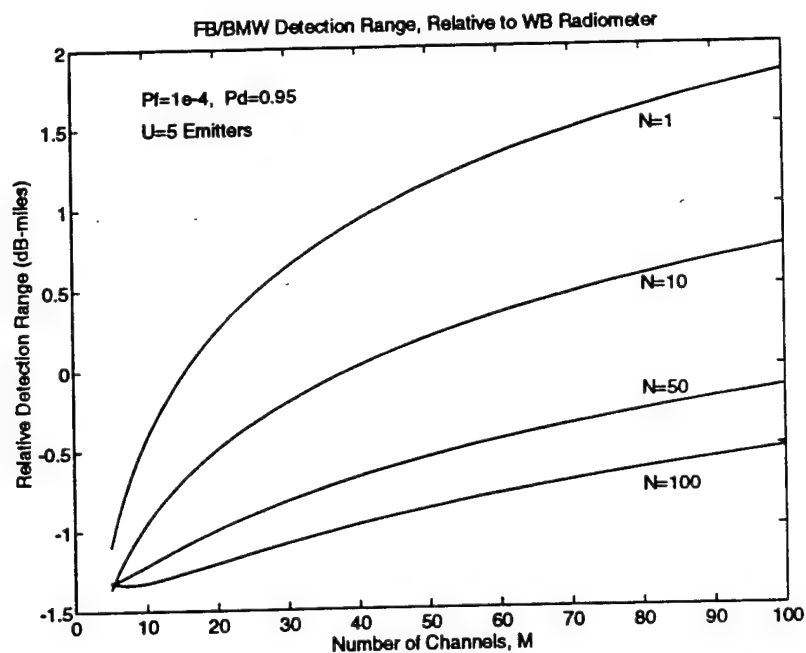
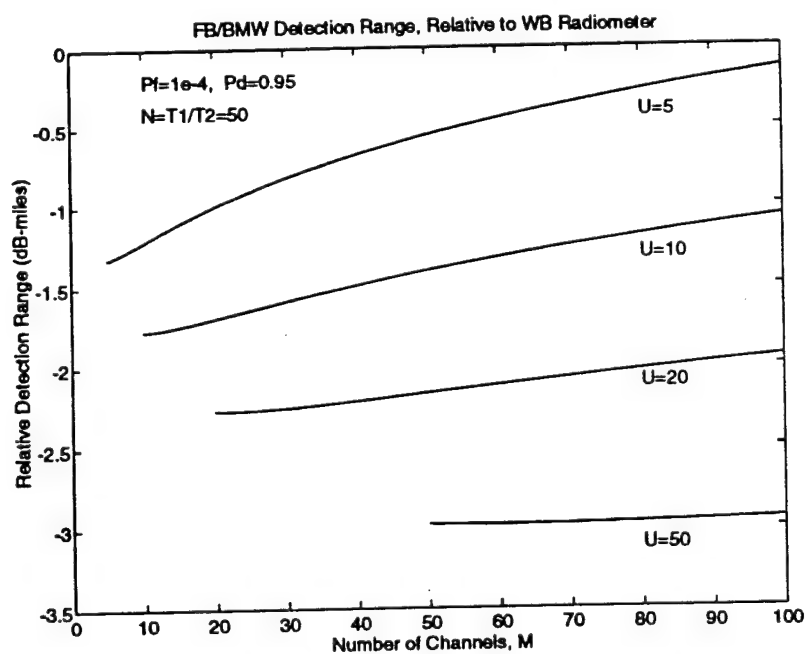Figure 4.14: Effect of Number of Channels on Detection Range, $U = 5$

Figure 4.15: Effect of Number of Channels on Detection Range, $N = 50$

4.3.4 Network Load

Clearly, adding more users increases the network's detectability for either detector. However, the radiometer uses the additional energy much more efficiently, as shown in Figure 4.16 and 4.17. When the number of emitters is small, the filter bank detector generally provides better detection performance than the radiometer, which is to be expected. However, as the network load increases, the radiometer becomes more sensitive. Furthermore, increases in M and N tend to decrease the load at which the two detectors provide equivalent performance.
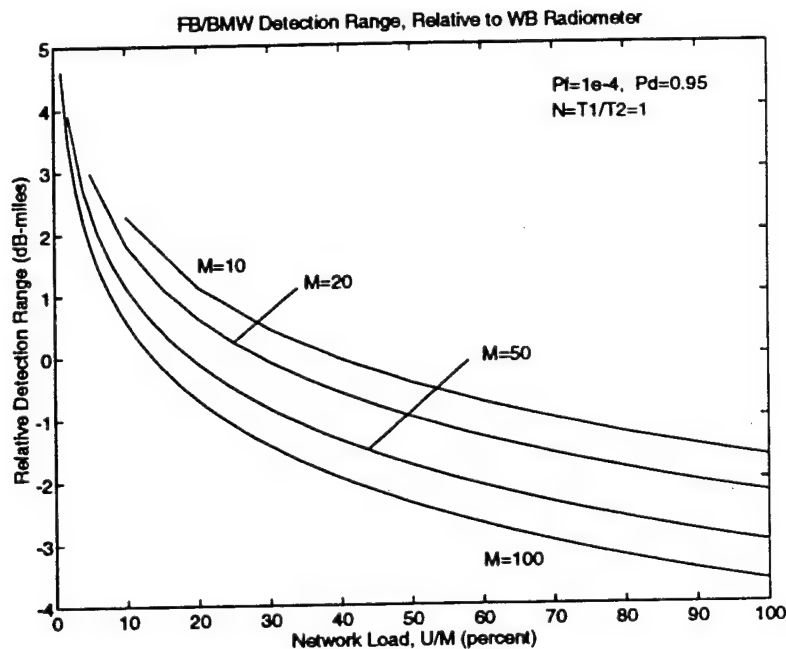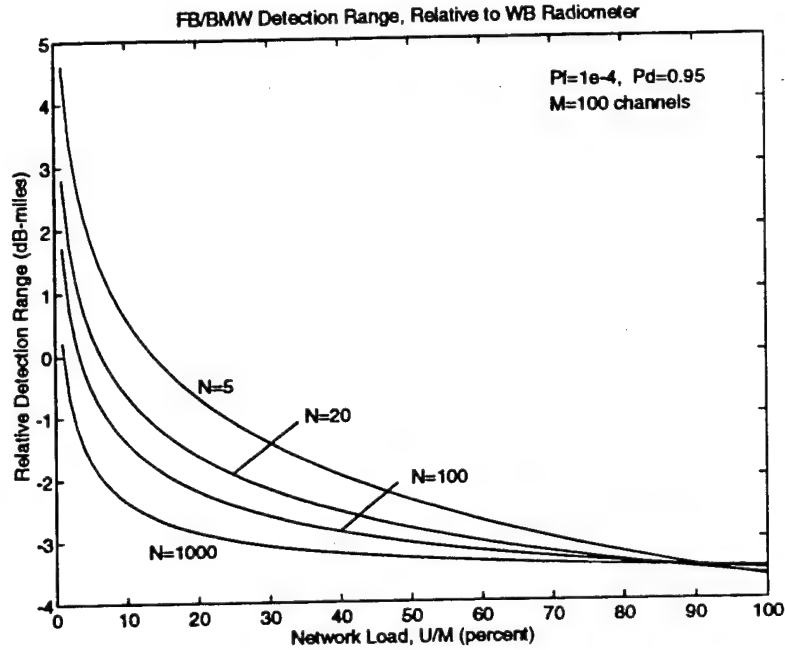

Figure 4.16: Effect of Network Load on Detection Range, $N = 1$

4.3.5 Wideband vs Channelized Detection

There are two primary reasons why the filter bank detection is superior only for detection of lightly-loaded networks. First, the FB/BMW detector is a sub-optimal detector originally conceived for the detection of single frequency hopping signals. Since FH

Figure 4.17: Effect of Network Load on Detection Range, $M = 100$

signals occupy only a single channel in any hop interval, the binary ORing of the channel outputs is appropriate. If signal energy is present in multiple channels, then a digital summation and thresholding of the filter bank outputs, as shown in Figure 3.7 and discussed in Section 3.3 is more sensitive—however, the interceptor must know how many signals might be present. If the threshold k_M is set too high, then networks containing just a few transmitters may go undetected.

If the binary OR operation is replaced with summing and thresholding, Equation (3.51) is modified as follows,

$$p_0 = \sum_{i=k_M}^{M} \binom{M}{i} Q_F^i (1 - Q_F)^{M-i} \tag{4.39}$$

The hop detection probability, p_1, is more difficult to solve, but an approximation is given in [0]:

$$p_1 = \sum_{i=k_M}^{M} \sum_{j=\max(0,i-M+U)}^{\min(i,U)} \binom{U}{j} \binom{M-U}{i-j} Q_D^j Q_F^{i-j}$$

$$(1 - Q_D)^{U-j}(1 - Q_F)^{M-i+j-U} \quad (4.40)$$

Q_F and Q_D are solved from the above equations, after p_0 and p_1 have been determined using Equations (3.49) and (3.50). It has been shown that $0.2U \leq k_M \leq 0.5U$ for maximum sensitivity [0]. Figure 4.18 shows the improvement which can be obtained if the interceptor has knowledge of the number of emitters and and builds the better detector.

A second reason why filter bank detection is inferior for large network loads is binary quantization loss—i.e., if the entire $T_1 \times W_1$ time-frequency space contains energy, a single energy measurement is more efficient than using NM separate measurements over $T_2 \times W_2$. This is illustrated in Figure 4.19. When $N = 1$, the quantization loss of 0.5 dB is attributed to frequency channelization. For $N > 1$, an additional 0.5 dB loss is incurred.
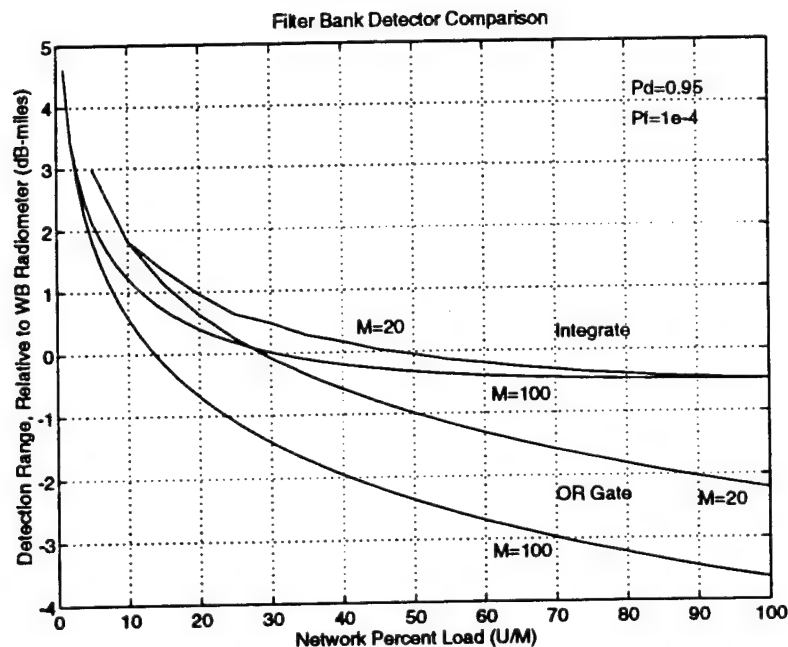

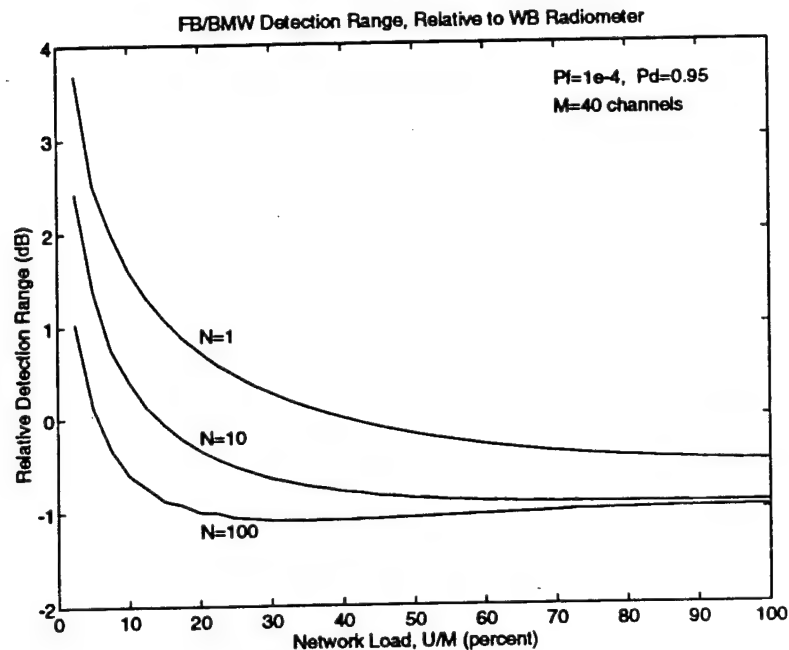Figure 4.18: Modified FB/BMW Detector Performance Comparison

Figure 4.19: Modified FB/BMW Performance as Function of N

4.3.6 Design Strategy

As seen in the preceding sections, the wideband radiometer generally the most threat to the LPI network. The FB/BMW detector is superior only when the hop rate is small and load are small. Changes in M and N do not affect the performance of the radiometer, since T_1 and W_1 are assumed fixed. Therefore, the LPI network waveforms should be designed such that detection with the radiometer is minimized. Then, M and N can be selected (perhaps based on the expected average number of users) such that the FB/BMW detector performs no better than the radiometer.

If the number of users changes significantly, the network parameters could be adapted to maintain equalization between the two receivers. This would require some form of network monitoring and control, which would track the number of active emitters and adjust M and N accordingly. Adaptive network control is beyond the scope of this research, although it has been investigated in [0].

4.4 Example Network Waveform Design

In this section, two candidate LPI networks are designed to illustrate the application of the waveform design techniques presented in Sections 4.2 and 4.3. First, the stand-off network intercept model will be used, followed by the dispersed network model. The design parameters given in Table 4.3 will be used.

$W_1 = 100$ MHz	total bandwidth
$T_1 = 1$ sec	signal duration
$U = 10$	number of users
$R_C = 5$ miles	broadcast range (equal power)
$P_E = 10^{-5}$	communication bit error probability
$R_b = 2400$ bps	data rate (2400 bits sent in T_1 interval)
$P_F = 10^{-4}$	interceptor false alarm probability
$P_D = 0.95$	interceptor detection probability
$G_I = 10$ dB, 0 dB	intercept gain for stand-off and dispersed network intercept scenarios, respectively

Table 4.3: Candidate Network Requirements

4.4.1 Stand-off Network Intercept Model

First, consider a simple DS-CDMA system in which BPSK modulation is used. To obtain $P_E = 10^{-5}$, $E_b/N_0 = 9.6$ dB, hence $S_C/N_0 = 43.4$ dB-Hz. The required SNR for a wideband radiometer tuned to the network is $S_I/N_0 = [Q^{-1}(P_F) - Q^{-1}(P_D)]\sqrt{W_1/T_1} = 47.3$ dB-Hz. Using these values with $U = 10$ and $G_I = 10$ dB, the network LPI quality factor is

$$Q_{RAD} = \left(\frac{R_C}{R_{RAD}}\right)^2 = \frac{(S_I/N_0)}{(S_C/N_0)}\frac{1}{UG_I}$$
$$= 47.3 - 43.4 - 10 - 10 = -16.1 \text{ dB}$$

Thus, the radiometer's intercept range is approximately 32 miles.

Now consider an FH-CDMA scheme using 32-ary orthogonal FSK waveforms and noncoherent detection. To transmit 2400 bps, a hop rate of $N/T_1 = 480$ hops/sec is required (there are $\log_2 32 = 5$ bits/hop). With $N = 480$ and $U = 10$, an appropriate

number of channels can be selected using the results from Section 4.3. As shown in Figure 4.12, the radiometer presents the greater threat, for all $M \leq 100$, so $M = 100$ will be used here. For $P_E = 10^{-5}$, $E_b/N_0 = 7.1$ dB, and $S_C/N_0 = 40.9$ dB-Hz. Therefore, the radiometer's quality factor is -13.6 dB—hence, using 32-ary FSK reduces the detection range to 24 miles.

The required SNR for the FB/BMW detector (with ORing of the channel outputs), is $S_I/N_0 = 41.5$ dB; its quality factor is then

$$Q_{FB} = \left(\frac{R_C}{R_{FB}}\right)^2 = \frac{(S_I/N_0)}{(S_C/N_0)} \frac{1}{G_I}$$
$$= 41.5 - 40.9 - 10 = -9.4 \text{ dB}$$

The FB/BMW detection range is therefore 14.8 miles, 2.1 dB smaller than that of the radiometer, which agrees with Figure 4.12.

Next, pulse combining is used in conjunction with Reed-Solomon coding to reduce the data rate. Using $L = 10$ with a $(31, 23)$ code results in $L_C/L = -8$ dB (from Figure 4.9) and a coding gain of $G_{code}(L) = 1.4$ dB (from Figure 4.11). From (4.35), $S_C/N_0 = 31.5$ dB-Hz, so $Q_{RAD} = -4.2$ dB, and $R_{RAD} \approx 8.1$ miles. For the FB/BMW detector, $Q_{FB} = 0$ dB, and $R_{FB} = R_C = 5$ miles.

The data rate could also be reduced by simply reducing the hop rate. Unlike pulse combining, which can be used independently by any network transmitter, this method requires all transmitters to change their hop rate simultaneously. Reducing the data rate to 240 bps decreases S_C/N_0 by 10 dB to 30.9 dB-Hz, and the new hop rate is 48 hops/sec. For the wideband radiometer, $Q_{LPI} = -3.6$ dB, and $R_{RAD} = 7.6$ miles. For the FB/BMW detector with $N = 48$, $S_I/N_0 = 39.4$ dB-Hz, hence $Q_{FB} = -1.5$ dB, and $R_{FB} = 6$ miles.

If a $(31, 23)$ Reed-Solomon code is used with the slower hop rate, $G_{code} = 2$ dB (from Figure 4.11 with $L = 1$). Therefore, the detection ranges for the two receivers decrease by 1 dB, yielding $R_{RAD} \approx 6$ miles, and $R_{FB} \approx 4.7$ miles.

Table 4.4 summarizes the results for the stand-off intercept scenario. Note that for these parameters, the radiometer's performance is better (its intercept range is larger) when pulse combining is used as opposed to the slower hop rate. This can be attributed to the noncoherent combining loss and reduced coding gain for $L = 10$: the difference in Q_{LPI} is $G_{code}(1) - G_{code}(10) - L_C = 2.6$ dB, resulting in a 1.3 dB range difference.

The FB/BMW detector's performance, on the other hand, is only slightly different for the two data rate reduction methods. As with the radiometer, noncoherent pulse combining is not as effective as slowing down the hop rate, although the difference is less pronounced because S_I/N_0 decreases as the hop rate decreases. As seen in Table 4.4, the 2.6 dB decrease in S_C/N_0 is offset by a 2.1 dB decrease in S_I/N_0, with an overall 0.5 dB reduction in Q_{FB}.

Comm Parameters	Radiometer	FB/BMW
BPSK modulation $S_C/N_0 = 43.4$ dB-Hz	$S_I/N_0 = 47.3$ dB-Hz $Q_{RAD} = -16.1$ dB $R_{RAD} = 32$ mi	
32-ary FSK $M = 100, N = 480$ $S_C/N_0 = 40.9$ dB-Hz	$S_I/N_0 = 47.3$ dB-Hz $Q_{RAD} = -13.6$ dB $R_{RAD} = 24$ mi	$S_I/N_0 = 41.5$ dB-Hz $Q_{FB} = -9.4$ dB $R_{FB} = 14.8$ mi
32-ary FSK $L = 10$ Pulse combining, $(31, 23)$ R-S code $M = 100, N = 480$ $L_C = 2$ dB, $G_{code}(L) = 1.4$ dB $S_C/N_0 = 31.5$ dB-Hz	$S_I/N_0 = 47.3$ dB-Hz $Q_{RAD} = -4.2$ dB $R_{RAD} = 8.1$ mi	$S_I/N_0 = 41.5$ dB-Hz $Q_{FB} = 0$ dB $R_{FB} = 5$ mi
32-ary FSK Reduced Hop Rate $M = 100, N = 48$ $S_C/N_0 = 30.9$ dB-Hz	$S_I/N_0 = 47.3$ dB-Hz $Q_{RAD} = -3.6$ dB $R_{RAD} = 7.6$ mi	$S_I/N_0 = 39.4$ dB-Hz $Q_{FB} = -1.5$ dB $R_{FB} = 6$ mi
32-ary FSK Reduced Hop Rate $(31, 23)$ R-S code $M = 100, N = 48$ $G_{code} = 2$ dB $S_C/N_0 = 28.9$ dB-Hz	$S_I/N_0 = 47.3$ dB-Hz $Q_{RAD} = -1.6$ dB $R_{RAD} = 6$ mi	$S_I/N_0 = 39.4$ dB-Hz $Q_{FB} = 0.5$ dB $R_{FB} = 4.7$ mi

Table 4.4: Stand-off Network Intercept Summary

4.4.2   Dispersed Network Intercept Model

The dispersed network intercept model calculations are summarized in Table 3.2. For this example, the transmitter locations, $\{(x_j, y_j)\}$ are uniformly distributed within a 10×10 mile region, each with broadcast range $R_C = 5$ miles. An omnidirectional intercept antenna is assumed.

To assess detectability with the wideband radiometer, the following parameters are input to the model: P_F, T_1, W_1, S_C/N_0, R_C, and the transmitter locations. The values of S_C/N_0 for the network structures given in the previous example will be used, i.e., $S_C/N_0 = 43.4$ dB-Hz for BPSK, 40.9 dB-Hz for 32-ary FSK, etc. Results are provided in Table 4.5 and Figures 4.20-4.22.

Comm Parameters	Detection Area (sq miles, $P_D = 0.95$)
BPSK modulation $S_C/N_0 = 43.4$ dB-Hz	WB Rad: 373.5
32-ary FSK $S_C/N_0 = 40.9$ dB-Hz	WB Rad: 232.1 FB/BMW: 153.9
32-ary FSK, combining, coding $S_C/N_0 = 31.5$ dB-Hz	WB Rad: 35.4 FB/BMW: 29.8
32-ary FSK, reduced hop rate $S_C/N_0 = 30.9$ dB-Hz	WB Rad: 29.2 FB/BMW: 49.2
32-ary FSK, reduced hop rate, coding $S_C/N_0 = 28.9$ dB-Hz	WB Rad: 15.4 FB/BMW: 32.4

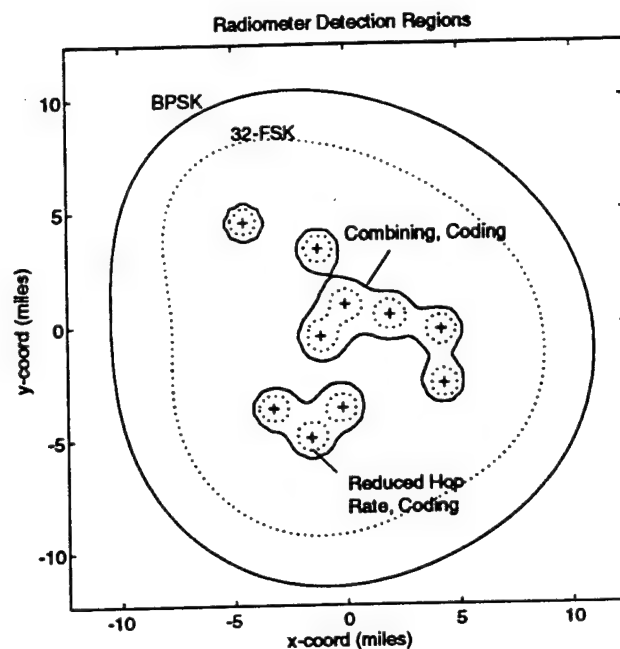Table 4.5: Dispersed Network Intercept Summary

Figure 4.20: Detectability Contours for the Wideband Radiometer
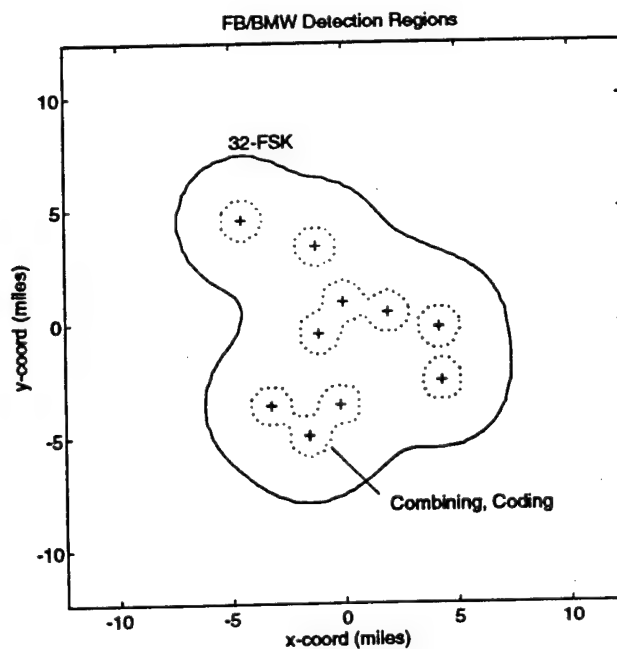

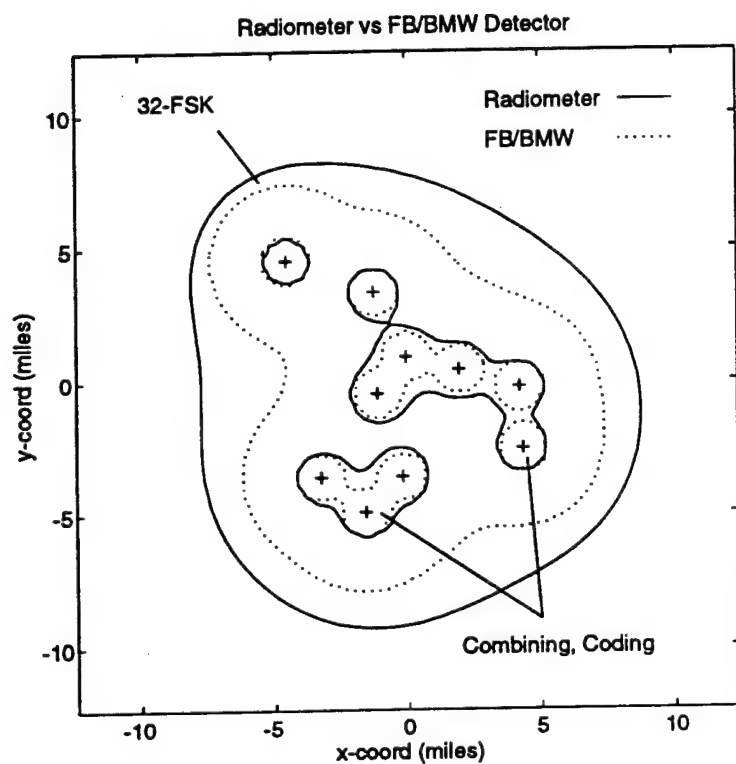Figure 4.21: Detectability Contours for the FB/BMW Detector

Figure 4.22: Comparison of Wideband Radiometer to FB/BMW Detector

Chapter 5

Conclusions

5.1 Summary

In Chapter 3, two network detectability models, with their corresponding performance metrics were developed. The dispersed network intercept model covers situations in which the network transmitters are geographically dispersed throughout the tactical region of interest, and the interceptor is inside the network. In this model, the achieved probability of detection is computed based on the received signal-to-noise ratio from each network transmitter. The performance metric for this model is the detection area (determined using numerical analysis techniques) for the specified probabilities of false alarm and detection. This model is highly dependent on the network scenario, such as transmitter placement.

The stand-off network intercept model is applicable for situations in which the network transmitters have equal power levels and are very close together, and the interceptor is relatively far away—resulting in roughly equal energy received from each emitter. Under these assumptions, the required SNR from each emitter can be determined as a function of the desired intercept performance, and network LPI quality factors can be used to directly compare the regions of communication and interception, as a function of the signal parameters. This model is scenario independent—only the waveform parameters and the methods used to detect them are important.

Several waveform design techniques for improving the covertness of the LPI network were developed in Chapter 4. Specific topics addressed were higher order M-ary

signaling, Reed-Solomon coding, and data rate control via pulse combining. When using these techniques in conjunction, significant reductions in network detectability can be obtained, as illustrated in examples for both the dispersed and stand-off intercept scenarios.

The network LPI quality factors were also used to illustrate how waveform parameters can be optimized to defeat channelized detectors, such as the filter bank/binary moving window detector. It was shown that the relative performance of the FB/BMW detector compared to the wideband radiometer is a function of the number of frequency channels, the hop rate, and the number of active transmitters. The radiometer generally presents the greater threat to the LPI network, since it forms a single detection decision based on the total received energy. The FB/BMW detector, on the other hand, combines many energy measurements into an overall decision, and is therefore susceptible to quantization losses.

It was shown that the FB/BMW detector is superior to the radiometer only when the frequency hop rate and number of active transmitters are small, and the number of frequency channels is large. If the interceptor has knowledge of how many users may be operating, the FB/BMW performance can be improved. However, for heavily loaded networks (i.e., all channels are in use), the wideband radiometer will always be superior, because of quantization losses in the FB/BMW detector.

5.2 Recommendations

Throughout the course of this research, several topics for further study became apparent. Some of these topics concern adding more detail to the detection models, while others deal with LPI networks in general. Topics for improving the detectability models derived here include the following:

- Incorporate the network detectability models into a computer aided analysis tool, such as the LPI/SDA program [0].

- Develop the appropriate detectability equations for other multiple access network schemes, such as the Joint Tactical Information Distribution System (JTIDS), and distributed time division multiple access (DTDMA).

- Incorporate more advanced intercept receivers, such as cyclic feature and hop rate detectors.

- Extend network detection models to allow mixed propagation modes, such as ground-to-ground, air-to-air, and ground-to-air.

- Integrate techniques for modeling realistic placement and/or movement of network transmitters (i.e., troop movement, strike force flight plans, etc.).

Potential topics regarding the administration of LPI networks include the study of adaptive power control and network control. Adaptive power control for LPI networks is critical to minimizing detectability and must address the problem of ensuring that each intended receiver has the required signal-to-noise ratio to demodulate the data stream with the specified probability of error.

Control of the LPI network also promises to be an interesting area of further research. Two levels of control will likely be required. Local control will be required at each network transmitter, while an overall network control function is desired to optimize the network's performance and minimize its detectability. Some issues to be considered are the adaptation of waveforms, power control, data rate control, and connectivity among various users. Any control algorithms should be as efficient as possible, thereby minimizing the required overhead.

Bibliography

[0] Abramowitz, M., and I.E. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs, and Mathematical Tables*, U.S. Department of Commerce, June 1964.

[0] Barton, D.K., "Simple Procedures for Radar Detection Calculations," *IEEE Transactions on Aerospace and Electronic Systems*, vol AES-5, pp. 837–846, September 1969.

[0] Chandler, E.W, and G.R. Cooper, "Development and Evaluation of an LPI Figure of Merit for Direct Sequence and Frequency Hop Systems," *Proceedings of the 1985 IEEE Military Communications Conference (MILCOM-85)*, October 1985.

[0] Chandler, E.W., and G.R. Cooper, "Direct-Sequence Interceptor Performance Gains due to a Partial Band Receiver Approach," *Proceedings of the 1986 IEEE Military Communications Conference (MILCOM-86)*, October 1986.

[0] Crepeau, P.J., "LPI and AJ Modulation Quality Factors," Naval Research Laboratory Memorandum Report NRL MR 3436, January 1977.

[0] Dillard, G.M., "A Moving-Window Detector for Binary Integration," *IEEE Transactions on Information Theory*, vol IT-13, January 1967.

[0] Dillard, R.A., "Detectability of Spread-Spectrum Signals," *IEEE Transactions on Aerospace and Electronic Systems*, vol 15, July 1979.

[0] Dillard, R.A., and G.M. Dillard, *Detectability of Spread-Spectrum Signals*, Artech House: Norwood, MA, 1989.

[0] Edell, J.D., "Wideband, Noncoherent, Frequency-Hopped Waveforms and their Hybrids in Low Probability of Intercept Communications," Naval Research Laboratory Report NRL 8025, 8 Nov 76.

[0] Engler, H.F., and D.H. Howard, "A Compendium of Analytic Models for Coherent and Non-Coherent Receivers," Air Force Wright Aeronautical Laboratory Technical Report AFWAL-TR-85-1118, September 1985.

[0] Gardner, W.A., and C.M. Spooner, "Signal Interception: Performance Advantages of Cyclic-Feature Detectors," Technical Report, Department of Electrical Engineering and Computer Science, University of California, Davis, April 1991.

[0] Gutman, L.L., and G.E. Prescott, "System Quality Factors for LPI Communication," *IEEE Aerospace and Electronic System Magazine*, pp. 25–28, December 1989.

[0] Longley, A.J., and P.L. Rice, "Prediction of Troposcatter Radio Transmission Loss Over Irregular Terrain, A Computer Method," Institute for Telecommunication Sciences, Boulder CO, NTIS AD-676 874, July 1968

[0] Mills, R.F., and G.E. Prescott, "Noncoherent Pulse Combining for Improved Multiple Access LPI Network Performance" *Proceedings of the 1993 IEEE Military Communications Conference (MILCOM-93)*, October 1993.

[0] Mills, R.F., and G.E. Prescott, "A Comparison of Various Radiometer Detection Models," submitted to *IEEE Transactions on Aerospace and Electronic Systems*, May 1993.

[0] Nicholson, D.L., *Spread Spectrum Signal Design: LPE and AJ Systems*, Computer Science Press: Rockville, MD, 1988.

[0] O'Brien, W.J., et.al. "On Achieving Network LPI for Spread Spectrum Communications," Army Research Office Technical Report ARO 21611.3-EL (NTIS AD-A163 985), E-Systems, Inc., Fairfax, VA, October 1985.

[0] Park, K.Y., "Performance Evaluation of Energy Detectors," *IEEE Transactions on Aerospace and Electronic Systems*, vol AES-14, March 1978.

[0] Prescott, G.E., and S. Francis, "Computer Aided Analysis of LPI Signal Detectability," *Proceedings of the 1991 IEEE Military Communications Conference (MILCOM-91)*, November 1991.

[0] Prescott, G.E., "Performance Metrics for Low Probability of Intercept Communication Systems," Technical Report, Grant #AFOSR-91-0018, Telecommunications and Information Sciences Laboratory, University of Kansas, October 1992.

[0] Proakis, J.G., *Digital Communications*, McGraw-Hill: New York, 1989.

[0] Sklar, B., *Digital Communications: Fundamentals and Applications*, Prentice-Hall: Englewood Cliffs, NJ, 1988.

[0] Torre, F., R. DiFazio, and E. German, "LPI Waveform Study," Rome Air Development Center Technical Report RADC-TR-90-24, April 1990.

[0] Torrieri, D.J., *Principles of Secure Communication Systems*, Artech House: Norwood, MA, 1992.

[0] Urkowitz, H., "Energy Detection of Unknown Deterministic Signals," *Proceedings of the IEEE*, vol 55, pp. 523–531, April 1967.

[0] Woodring, D., and J. Edell, "Detectability Calculation Techniques," Naval Research Laboratory Report NRL 5480, 1 Sep 1977.